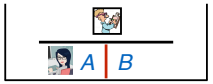
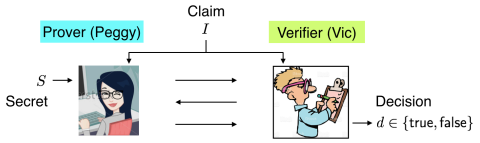
# Zero-Knowledge Protocols






## The People

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser MIT — Silvio Micali MIT — Charles Rackoff University of Toronto

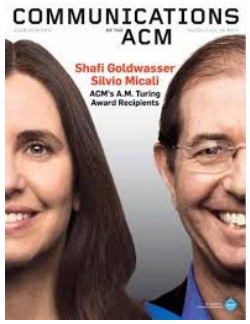
on

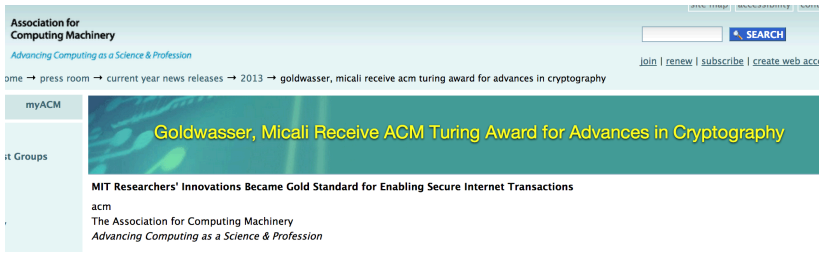
st part of the paper we introduce a

We propose to classify languages according to the amount of additional knowledge that must be

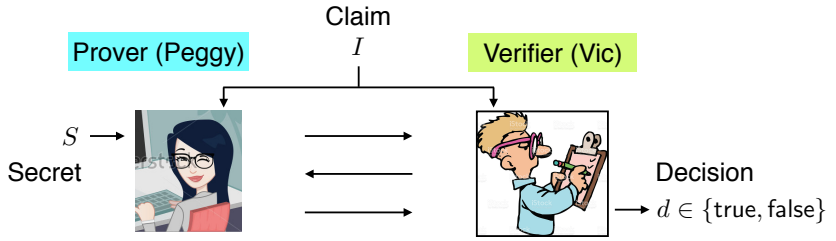


## The Awards



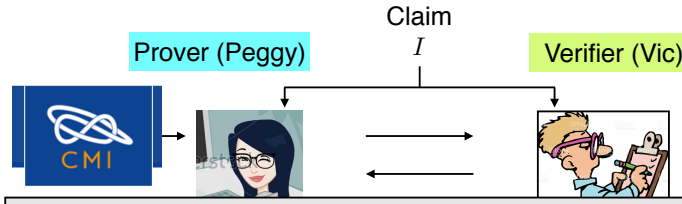



A zero-knowledge protocol allows Peggy to

- Convince Vic that her claim is true and that she knows $S$
- Without revealing anything beyond that

| Peggy | Vic | Claim *I* | Secret *S* |
|---|---|---|---|
| Student | Another student | I know how to solve the homework problem | Peggy's solution |
| An Internet user | A server | I have a valid password | the password |
| Mathematician | The Clay Institute | I have a proof that **P** is not equal to **NP** | The proof |

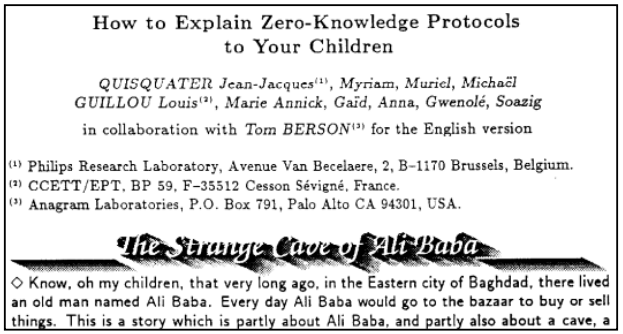



The Clay Mathematics Institute (CMI) has named seven "Millennium Prize Problems." The Scientific Advisory Board of CMI (SAB) selected these problems, focusing on important classic questions that have resisted solution over the years. The Board of Directors of CMI designated a $7 million prize fund for the solutions to these problems, with $1 million allocated to each. The Directors of CMI, and no other persons or body, have the authority to authorize payment from this fund or to modify or interpret these stipulations. The Board of Directors of CMI makes all mathematical decisions for CMI, upon the recommendation of its SAB.

| Peggy | Vic | Claim *I* | Secret *S* |
|---|---|---|---|
| Student | Another student | I know how to solve the homework problem | Peggy's solution |
| An Internet user | A server | I have a valid password | the password |
| Mathematician | The Clay Institute | I have a proof that **P** is not equal to **NP** | The proof |



## Ali-Baba's Zero-Knowledge Protocol



How to Explain Zero-Knowledge Protocols to Your Children

*QUISQUATER Jean-Jacques[1], Myriam, Muriel, Michaël*
*GUILLOU Louis[2], Marie Annick, Gaïd, Anna, Gwenolé, Soazig*
in collaboration with *Tom BERSON[3]* for the English version

[1] Philips Research Laboratory, Avenue Van Becelaere, 2, B-1170 Brussels, Belgium.
[2] CCETT/EPT, BP 59, F-35512 Cesson Sévigné, France.
[3] Anagram Laboratories, P.O. Box 791, Palo Alto CA 94301, USA.

*The Strange Cave of Ali Baba*

◇ Know, oh my children, that very long ago, in the Eastern city of Baghdad, there lived an old man named Ali Baba. Every day Ali Baba would go to the bazaar to buy or sell things. This is a story which is partly about Ali Baba, and partly also about a cave, a

This story is used to explain zero-knowledge in many places.
Including Wikipedia.
But it doesn't make a lot of sense.
We will use Joseph Jaeger's variant.



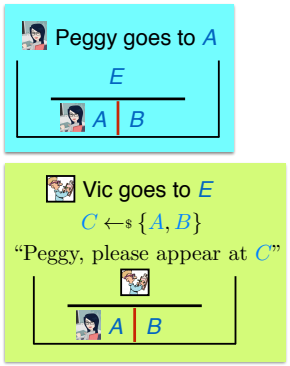
## Ali Baba's ZK Protocol

$\mathrm{MW}[A, B]$ = Magic Words opening the $A \to B$ portal
$\mathrm{MW}[B, A]$ = Magic Words opening the $B \to A$ portal

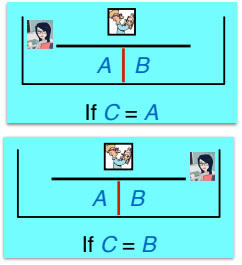
Peggy has secret $S \in \{\mathrm{MW}[A, B], \mathrm{MW}[B, A]\}$

Peggy does not want Vic to know which of the two magic words she has.

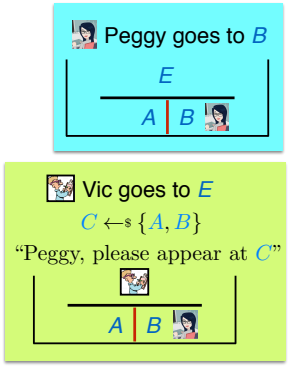
**If Peggy knows MW[*A*,*B*] :**




Final step, in either case:

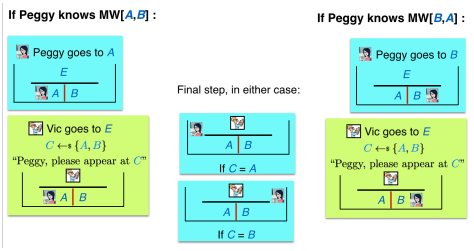



**If Peggy knows MW[*B*,*A*] :**





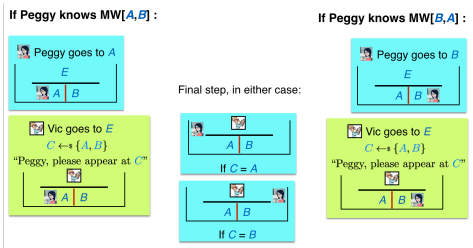

## Ali Baba's ZK Protocol




**Completeness:** If Peggy's claim is true, meaning she knows either MW[*A*,*B*] or MW[*B*,*A*], and both parties follow the protocol, then Vic will accept.

**Why?** Peggy can appear at whatever side Vic requests.

## Ali Baba's ZK Protocol



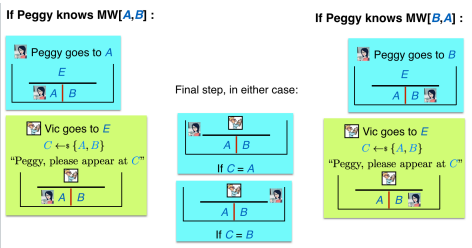

**Completeness:** If Peggy's claim is true, meaning she knows either MW[$A$,$B$] or MW[$B$,$A$], and both parties follow the protocol, then Vic will accept.

**Soundness**: If Peggy's claim is false, meaning she knows neither MW[$A$,$B$] nor MW[$B$,$A$], then Vic will reject with probability at least 1/2, even if Peggy cheats, meaning does not follow the prescribed protocol.

**Why?** Cheating Peggy can start at any $X \in \{A, B\}$ of her choice, but Vic picks $C$ at random and cheating Peggy cannot appear at $C \neq X$.



## Ali Baba's ZK Protocol




**Completeness:** If Peggy's claim is true, meaning she knows either MW[$A$,$B$] or MW[$B$,$A$], and both parties follow the protocol, then Vic will accept.

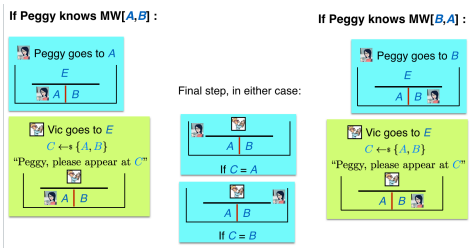
**Soundness**: If Peggy's claim is false, meaning she knows neither MW[$A$,$B$] nor MW[$B$,$A$], then Vic will reject with probability at least 1/2, even if Peggy cheats, meaning does not follow the prescribed protocol.

**Zero-knowledge**: If Peggy's claim is true, and Peggy follows the protocol, then Vic will not learn which of the two secrets MW[$A$,$B$], MW[$B$,$A$] Peggy knows.

**Why?** Regardless of the secret, Vic sees Peggy appearing at whatever side he requests.



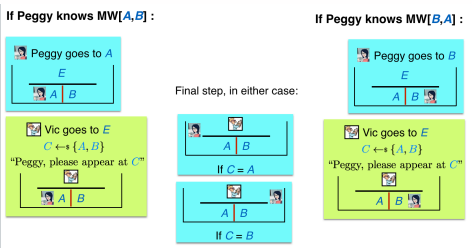
## Ali Baba's ZK Protocol




| | Pegg's claim is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | TRUE | honest | always accept |
| Soundness | FALSE | cheating | accept with probability at most 1/2 |
| Zero-knowledge | TRUE | honest | not learn which of the two secrets Peggy knows |



## Ali Baba's ZK Protocol




| | Pegg's claim is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | TRUE | honest | always accept |
| Soundness | FALSE | cheating | accept with probability at most 1/2 |
| Zero-knowledge | TRUE | honest | not learn which of the two secrets Peggy knows |

This story may not make complete sense.
To make zero-knowledge sensible, we need DEFINITIONS.
The definitions are intriguing: how can one mathematically capture the ``knowledge'' learned by interacting with another party?

# Zero-knowledge protocol for Quadratic Residuosity



## Some math definitions

Let $N \geq 1$ be an integer. We say that $x \in \mathbb{Z}_N^*$ is a square-root of $X \in \mathbb{Z}_N^*$ modulo $N$ if $x^2 \bmod N = X$. We say that $X \in \mathbb{Z}_N^*$ is a square, or quadratic residue, modulo $N$, if it has a square root modulo $N$.

$\mathsf{SR}(N, X) = \{x \in \mathbb{Z}_N^* : X = x^2 \bmod N\}$ The set of square roots of $X$ modulo $N$

$\mathsf{QR}(N) = \{X \in \mathbb{Z}_N^* : \mathsf{SR}(N, X) \neq \emptyset\}$ The set of quadratic residues modulo $N$

$\mathsf{QR} = \{(N, X) : N \geq 1 \text{ and } X \in \mathsf{QR}(N)\}$ . The language of quadratic residues

**Example:** Let $N = 11$.

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $x^2 \bmod 11$ | 1 | 4 | 9 | 5 | 3 | 3 | 5 | 9 | 4 | 1 |

$\mathsf{SR}(11, 5) = \{4, 7\}$
$\mathsf{SR}(11, 6) = \emptyset$
$\mathsf{QR}(11) = \{1, 3, 4, 5, 9\}$

**Fact:** Let $X \in \mathbb{Z}_N^*$. Then $X \in \mathsf{QR}(N)$ if and only if $X^{-1} \bmod N \in \mathsf{QR}(N)$.

**Fact:** Let $x, X \in \mathbb{Z}_N^*$. Then $x \in \mathsf{SR}(N, X)$ if and only if $x^{-1} \bmod N \in \mathsf{SR}(N, X^{-1} \bmod N)$.



## Complexity of QR

$\mathsf{SR}(N, X) = \{x \in \mathbb{Z}_N^* : X = x^2 \bmod N\}$ The set of square roots of $X$ modulo $N$

$\mathsf{QR}(N) = \{X \in \mathbb{Z}_N^* : \mathsf{SR}(N, X) \neq \emptyset\}$ The set of quadratic residues modulo $N$

$\mathsf{QR} = \{(N, X) : N \geq 1 \text{ and } X \in \mathsf{QR}(N)\}$ . The language of quadratic residues

**Input:** *(N,X)*
**Question:** Is *(N,X)* in QR?

**Input:** *(N,X)* in QR
**Find:** A square root *x* of *X* modulo *N*

These problems are **hard**: There are no (known) efficient (polynomial-time) algorithms for them.

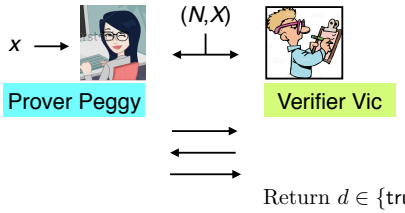
But **easy** in some cases: There are polynomial-time algorithms when *N* is prime.

**Input:** *N*
**Find:** Some *X* in QR(*N*)

This is **easy**: Pick $x \leftarrow\!\!\$\ \mathbb{Z}_N^*$ and return $X \leftarrow x^2 \bmod N$.



## Proving quadratic residuosity



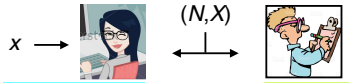

Both parties have (*N*,*X*), the common input
Peggy claims that (*N*,*X*) is in QR.
Peggy has *x* such that $x^2 \bmod N = X$

Definition: Vic **accepts** if $d = \text{true}$

The protocol is the prescribed, shown steps for the parties. A party can follow the protocol (it is honest) or not (it is cheating). Vic is **always honest**, but not so Peggy.

| | (*N*,*X*) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | accept with probability at most 1/2 |
| Zero-knowledge | in QR | honest | not learn *x* |

## A non-ZK protocol



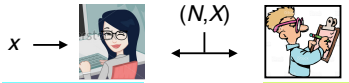

Peggy has $x$ such that $x^2 \bmod N = X$

$\text{Cmt} \leftarrow x$ — Cmt → — $d \leftarrow (\text{Cmt}^2 \bmod N = X)$ ; Return $d$

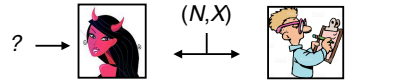
| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |



## A non-ZK protocol




$\text{Cmt} \leftarrow x$ — Cmt → — $d \leftarrow (\text{Cmt}^2 \bmod N = X)$ ; Return $d$




$\text{Cmt} \leftarrow ?$ — Cmt → — $d \leftarrow (\text{Cmt}^2 \bmod N = X)$ ; Return $d$

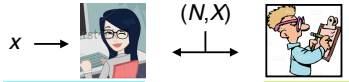
**Soundness: Peggy is cheating**

But $X \notin \text{QR}(N)$ means there does not exist Cmt such that $\text{Cmt}^2 \bmod N = X$, so Vic will return $d$ = false.

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | never accept |



## A non-ZK protocol




Peggy has $x$ such that $x^2 \bmod N = X$

$\text{Cmt} \leftarrow x$ — Cmt → — $d \leftarrow (\text{Cmt}^2 \bmod N = X)$ ; Return $d$

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | never accept |
| Zero-knowledge | in QR | honest | learn $x$, so ZK fails |



## Splitting

Suppose we split up $X$ as: $\boxed{X = \text{Cmt} \cdot Y \bmod N}$ for some $\text{Cmt}, Y \in \mathbb{Z}_N^*$

Then we have:

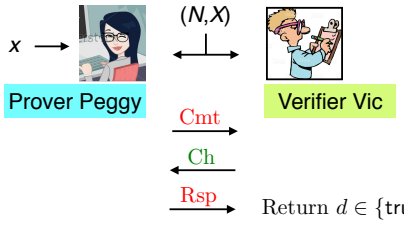
**Fact:**
- If ($\text{Cmt} \in \text{QR}(N)$ and $Y \in \text{QR}(N)$) then $X \in \text{QR}(N)$
- If $X \notin \text{QR}(N)$ then ($\text{Cmt} \notin \text{QR}(N)$ or $Y \notin \text{QR}(N)$)

**Proof Intuition:**

$$\sqrt{\text{Cmt}} \cdot \sqrt{Y} = \sqrt{\text{Cmt} \cdot Y} = \sqrt{X}$$

**Proof, formally:**

We are given that $\text{Cmt} \in \text{QR}(N)$, so $\text{Cmt} = c^2 \bmod N$ for some $c \in \mathbb{Z}_N^*$
We are given that $Y \in \text{QR}(N)$, so $Y = y^2 \bmod N$ for some $y \in \mathbb{Z}_N^*$
Let $w = cy \bmod N$
Then $w^2 \bmod N = c^2 y^2 \bmod N = \text{Cmt} \cdot Y \bmod N$
But we are given that $\text{Cmt} \cdot Y \bmod N = X$
So $w^2 \bmod N = X$
So $X \in \text{QR}(N)$




## Splitting for zero knowledge

Both parties have (N,X)
Peggy claims that (N,X) is in QR.
Peggy has $x$ such that $x^2 \bmod N = X$
Peggy does not want to reveal $x$

Peggy splits up $X$ as: $\boxed{X = \text{Cmt} \cdot Y \bmod N}$ for some $\text{Cmt}, Y \in \mathbb{Z}_N^*$

Then she makes two claims:

**Claim 0:** $\text{Cmt} \in \text{QR}(N)$
**Claim 1:** $Y \in \text{QR}(N)$

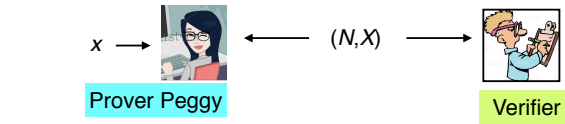
Vic picks a bit Ch at random and asks:
Peggy, please prove Claim Ch

**Soundness:** If $X$ is not in QR(N) then one of the two Claims is false, so Vic rejects with probability at least 1/2

**ZK:** Rsp does not reveal a square root of $X$

If $\text{Ch} = 0$ then Peggy sends $\text{Rsp} = \sqrt{\text{Cmt}}$
If $\text{Ch} = 1$ then Peggy sends $\text{Rsp} = \sqrt{Y}$





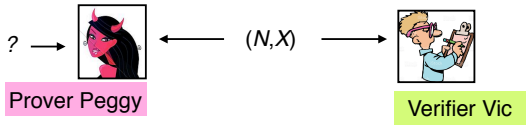

## The ZK protocol for QR

$c \leftarrow\!\!\$\ \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt →
← Ch — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$
$\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp →
$d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

$$\begin{aligned}\text{Rsp}^2 \bmod N &= (c^{-1} \cdot x^{\text{Ch}})^2 \bmod N \\ &= (c^2)^{-1} \cdot (x^2)^{\text{Ch}} \bmod N \\ &= \text{Cmt}^{-1} \cdot X^{\text{Ch}} \bmod N\end{aligned}$$

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |





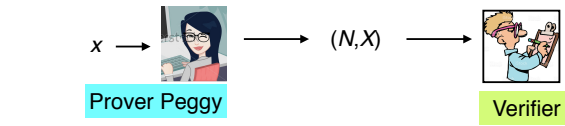

## Soundness

$\text{Cmt} \leftarrow ?$ — Cmt →
← Ch — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$
$\text{Rsp} \leftarrow ?$ — Rsp →
$d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

Let $Y = \text{Cmt}^{-1} \cdot X \bmod N$, so that $X = \text{Cmt} \cdot Y \bmod N$
By assumption $X \notin \text{QR}(N)$
So by Fact either $\text{Cmt} \notin \text{QR}(N)$ or $Y \notin \text{QR}(N)$
So $d =$ false with probability at least 1/2

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | accept with probability at most 1/2 |



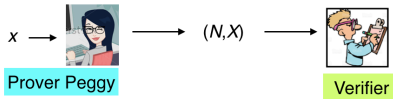



## The ZK protocol for QR

$c \leftarrow\!\!\$\ \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt →
← Ch — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$
$\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp →
$d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

$\text{Rsp} = c^{-1} x^{\text{Ch}} \bmod N$ is a random square root of the random square $\text{Cmt}^{-1} \cdot X^{\text{Ch}} \bmod N$

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | accept with probability most 1/2 |
| Zero-knowledge | in QR | honest | learn nothing more about $x$ than he knew before |




**The ZK protocol for QR**

$c \leftarrow_{\$} \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt →

← Ch — $\text{Ch} \leftarrow_{\$} \{0,1\}$

$\text{Rsp} \leftarrow c^{-1} x \bmod N$ — Rsp →

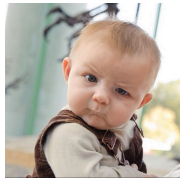
$d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X \pmod N)$ ; Return $d$

| | (N,X) is | Peggy is | Vic will |
|---|---|---|---|
| Completeness | in QR | honest | always accept |
| Soundness | not in QR | cheating | accept with probability most 1/2 |
| Zero-knowledge | in QR | honest | learn nothing more about *x* than he knew |

But what exactly does it mean that this protocol is zero knowledge?
Next we give a DEFINITION and show that it is met.

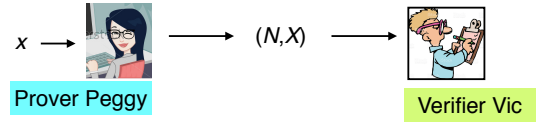


# Defining and proving ZK for Quadratic Residuosity



**Note for experts:** What we define here is honest-verifier, perfect zero knowledge for the QR protocol.






**Transcripts**

$c \leftarrow_{\$} \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt →

← Ch — $\text{Ch} \leftarrow_{\$} \{0,1\}$

$\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp →

$d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

---

The protocol is captured by the pair $(P, V)$ of algorithms describing the behavior of the prover and verifier depicted above. We want to define what it means for this pair to be zero-knowledge for the language QR.

A protocol transcript is a possible sequence $(\text{Cmt}, \text{Ch}, \text{Rsp})$ of messages exchanged.

$\underline{\text{Tr}_{(P,V)}((N,X),x)}$ ← This algorithm generates transcripts
$c \leftarrow_{\$} \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$
$\text{Ch} \leftarrow_{\$} \{0,1\}$
$\text{Rsp} \leftarrow c^{-1} x^{\text{Ch}} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

**Note:** The algorithm takes the secret *x* as input to do this!



$\underline{\text{Tr}_{(P,V)}((N,X),x)}$ ← This algorithm generates transcripts
$c \leftarrow_{\$} \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$
$\text{Ch} \leftarrow_{\$} \{0,1\}$
$\text{Rsp} \leftarrow c^{-1} x^{\text{Ch}} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

We call these transcripts real
The algorithm takes the secret *x* as input

**Simulation**

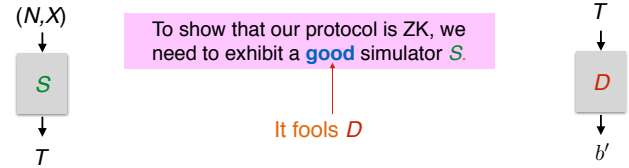
**ZK Intuition:** The information conveyed by the protocol is the transcript *T*.

**ZK definition idea:** (*P*,*V*) is zero knowledge if a transcript *T*, that looks just like a real one, can be (efficiently) generated, given (*N*,*X*) **but not given** *x*.

**Two new members of the cast of characters**

**Simulator *S***
Takes input (*N*,*X*) and generates a transcript *T* that is supposed to look like a real one. *S* does NOT get input *x*!

**Distinguisher *D***
Takes input *T* and tests whether *T* was generated by Tr or by *S*



Let $(P,V)$ be the prover-verifier pair defining the protocol.
Let $S$ be a candidate simulator.

## Simulation

**Game** $\text{ZK}_{(P,V),S}$

| Initialize | Transcript$((N,X),x)$ |
|---|---|
| $b \leftarrow\$ \{0,1\}$ | If $(x^2 \bmod N \neq X)$ then return $\perp$ |
| Finalize$(b')$ | If $(b=1)$ then $T \leftarrow\$ \mathsf{Tr}_{(P,V)}((N,X),x)$ |
| Return $(b'=b)$ | Else $T \leftarrow\$ S((N,X))$ |
| | Return $T$ |

The adversary playing this game is the distinguisher $D$.

Probability that the game returns true when run with adversary $D$

$$\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 2 \cdot \overbrace{\Pr[\text{ZK}^{D}_{(P,V),S}]}^{} - 1$$

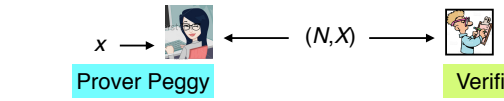
**Def:** $S$ is a *zk simulator* (good!) for $(P,V)$ over QR if $\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 0$ for all distinguishers $D$.

**Def:** $(P,V)$ is a zero-knowledge protocol for language QR if there exists an efficient zk simulator $S$ for $(P,V)$ over QR.

Polynomial time, in length of input to $S$
Here, $\mathcal{O}(k^3)$, where $k$ is the length of $N$

To show that our protocol is ZK, we need to exhibit an efficient zk simulator $S$.






## A simulator for the QR protocol?

$c \leftarrow\$ \mathbb{Z}^*_N$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — ← Ch — $\text{Ch} \leftarrow\$ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

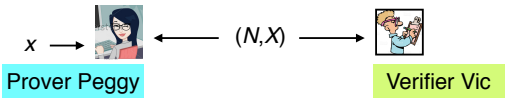
**Task:** Exhibit an efficient simulator $S$ such that $\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 0$ for all distinguishers $D$.

$S((N,X))$ must return $T = (\text{Cmt}, \text{Ch}, \text{Rsp})$ such that $\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N$.

Simulator $S_2((N,X))$
$x \leftarrow\$ \mathsf{SR}(N,X)$ ← This operation cannot be efficiently performed.
$T \leftarrow\$ \mathsf{Tr}_{(P,V)}((N,X),x)$
Return $T$

| zk simulator? | Efficient? |
|---|---|
| Yes | No |






## A simulator for the QR protocol?

$c \leftarrow\$ \mathbb{Z}^*_N$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — ← Ch — $\text{Ch} \leftarrow\$ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

**Task:** Exhibit an efficient simulator $S$ such that $\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 0$ for all distinguishers $D$.

$S((N,X))$ must return $T = (\text{Cmt}, \text{Ch}, \text{Rsp})$ such that $\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N$.

Simulator $S_0((N,X))$
$c \leftarrow\$ \mathbb{Z}^*_N$ ; $\text{Cmt} \leftarrow c^2 \bmod N$
$\text{Ch} \leftarrow 0$ ; $\text{Rsp} \leftarrow c^{-1} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

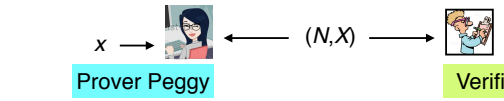
**Check:**

$$\begin{aligned} \text{Cmt}^{-1} \cdot X^{\text{Ch}} \bmod N &= (c^2)^{-1} \cdot X^0 \bmod N \\ &= (c^{-1})^2 \bmod N \\ &= \text{Rsp}^2 \bmod N \end{aligned}$$

Looking good … ? But we always have Ch = 0 !

| zk simulator? | Efficient? |
|---|---|
| ? | Yes |






## A simulator for the QR protocol?

$c \leftarrow\$ \mathbb{Z}^*_N$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — ← Ch — $\text{Ch} \leftarrow\$ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

**Task:** Exhibit an efficient simulator $S$ such that $\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 0$ for all distinguishers $D$.

$S((N,X))$ must return $T = (\text{Cmt}, \text{Ch}, \text{Rsp})$ such that $\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N$.

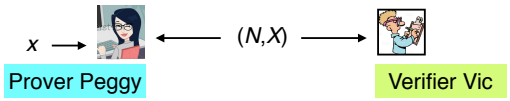
Simulator $S_0((N,X))$
$c \leftarrow\$ \mathbb{Z}^*_N$ ; $\text{Cmt} \leftarrow c^2 \bmod N$
$\text{Ch} \leftarrow 0$ ; $\text{Rsp} \leftarrow c^{-1} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

Attack:

Distinguisher $D$
$T \leftarrow\$ \text{Transcript}((11,9))$
$(\text{Cmt}, \text{Ch}, \text{Rsp}) \leftarrow T$
If $(\text{Ch} = 0)$ then return 0 else return 1

$\mathbf{Adv}^{\text{zk}}_{(P,V),S_0}(D) = 1/2$

| zk simulator? | Efficient? |
|---|---|
| No | Yes |




**A simulator for the QR protocol!**

$c \leftarrow\!\!\$\ \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — Ch ← — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

**Task:** Exhibit an efficient simulator $S$ such that $\mathbf{Adv}^{\text{zk}}_{(P,V),S}(D) = 0$ for all distinguishers $D$.

$S((N,X))$ must return $T = (\text{Cmt}, \text{Ch}, \text{Rsp})$ such that $\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N$.

Simulator $S((N,X))$
$\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ ; $\text{Rsp} \leftarrow\!\!\$\ \mathbb{Z}_N^*$
$\text{Cmt} \leftarrow \text{Rsp}^{-2} \cdot X^{\text{Ch}} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

**Check:**

$$\begin{aligned}\text{Cmt}^{-1} \cdot X^{\text{Ch}} \bmod N &= (\text{Rsp}^{-2} \cdot X^{\text{Ch}})^{-1} \cdot X^{\text{Ch}} \bmod N \\ &= \text{Rsp}^2 \cdot X^{-\text{Ch}} \cdot X^{\text{Ch}} \bmod N \\ &= \text{Rsp}^2 \bmod N\end{aligned}$$

Looking good … ? And it is good …

| zk simulator? | Efficient? |
|---|---|
| Yes | Yes |






**A simulator for the QR protocol!**

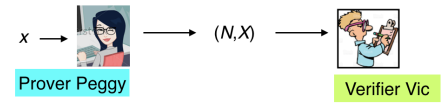
$c \leftarrow\!\!\$\ \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — Ch ← — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} \cdot x^{\text{Ch}} \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X^{\text{Ch}} \pmod N)$ ; Return $d$

The trick is for the simulator to pick the components of the transcript out of order: first it picks Ch, Rsp and then it computes Cmt to match.

Simulator $S((N,X))$
$\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ ; $\text{Rsp} \leftarrow\!\!\$\ \mathbb{Z}_N^*$
$\text{Cmt} \leftarrow \text{Rsp}^{-2} \cdot X^{\text{Ch}} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

| zk simulator? | Efficient? |
|---|---|
| Yes | Yes |






**The ZK protocol for QR**

$c \leftarrow\!\!\$\ \mathbb{Z}_N^*$ ; $\text{Cmt} \leftarrow c^2 \bmod N$ — Cmt → — Ch ← — $\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ — $\text{Rsp} \leftarrow c^{-1} x \bmod N$ — Rsp → — $d \leftarrow (\text{Rsp}^2 \equiv \text{Cmt}^{-1} \cdot X \pmod N)$ ; Return $d$

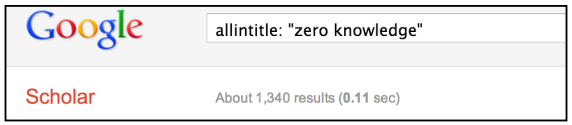
Simulator $S((N,X))$
$\text{Ch} \leftarrow\!\!\$\ \{0,1\}$ ; $\text{Rsp} \leftarrow\!\!\$\ \mathbb{Z}_N^*$
$\text{Cmt} \leftarrow \text{Rsp}^{-2} \cdot X^{\text{Ch}} \bmod N$
$T \leftarrow (\text{Cmt}, \text{Ch}, \text{Rsp})$
Return $T$

We gave a definition of what it means for the above protocol to be ZK.
To show that this definition was met, we exhibited the above simulator.



**Zero-knowledge beyond Quadratic Residuosity**

## Research





Research on zero-knowledge protocols

- **Considers different forms:** perfect, statistical, computational, concurrent, malleable, non-malleable, reset-secure, non-interactive, succinct, …
- **Gives lots of protocols:** For NP languages, for graph non-isomorphism, for PSPACE, with constant rounds, …



## Utility?

In theory, zero-knowledge has lots of applications.
Much recent work on efficient implementations.
In systems for anonymous credentials and smart contracts.
People who work on it like to claim it is practical.

But in practice, usage is limited. → WHY?

Not everything cool is actually useful.
We have other, more practical ways to solve real problems.