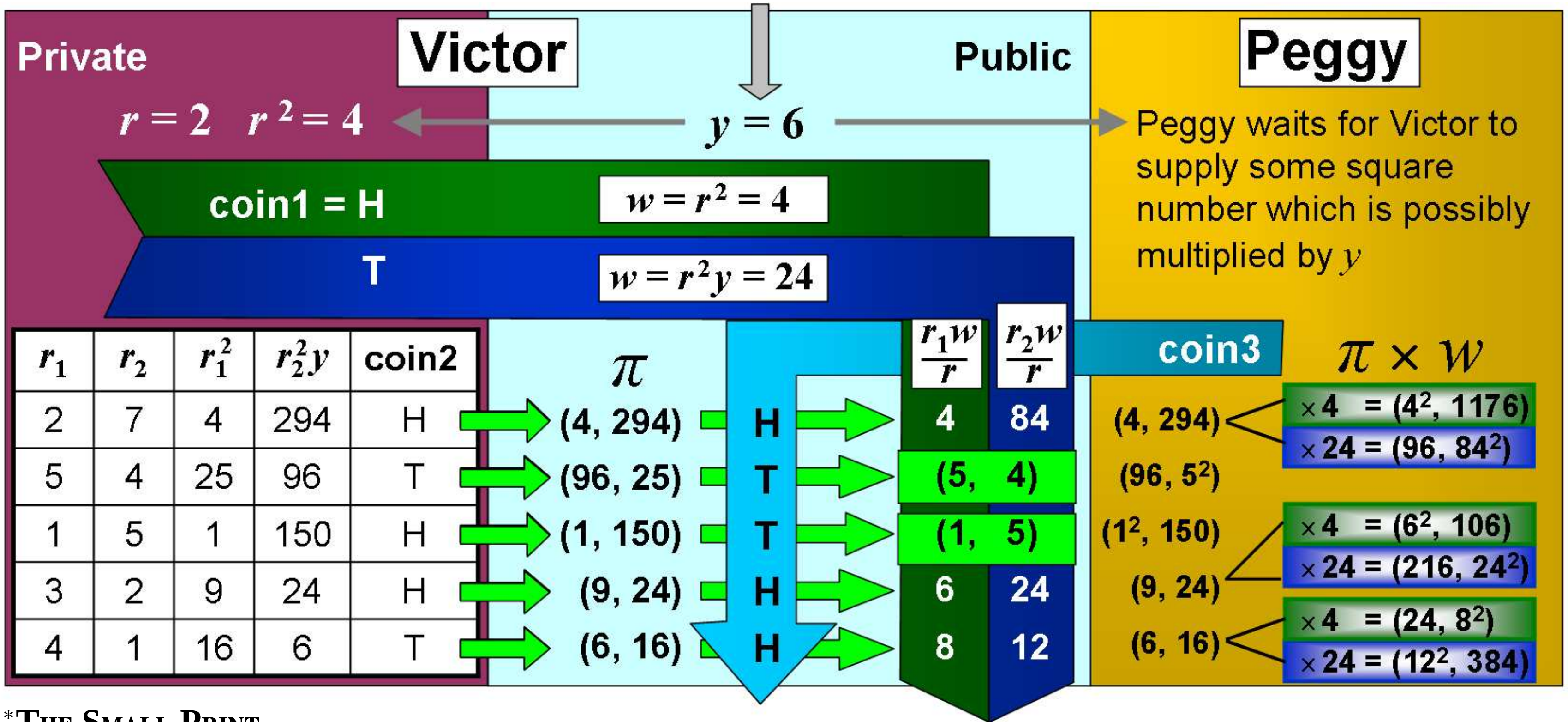
THEOREM OF THE DAY

Quadratic Nonresidue is Zero-Knowledge Provable *There exists a protocol whereby an oracle, given positive integers $x < y$, y coprime to x, can respond Yes or No to the question "Is y a quadratic nonresidue mod x?" and impart no other information that is not polynomial-time computable from x and y.*

To check if $z^2 = y \bmod x$ for some $z < x$, that is, to check if y is a quadratic residue or a quadratic nonresidue, appears to be as hard as factoring x. The protocol described below and illustrated on the right is probabilistically polynomial for quadratic nonresidue. To simplify notation 'quadratic nonresidue' is replaced by 'square root'.

The Basic Idea*

Victor (the 'verifier') can compute squares but not square roots. The (mathematically) omniscient Peggy (the 'prover') will reveal whether or not y is a square number. Victor secretly chooses a random integer r and tosses a coin. If the coin is Heads he shows Peggy $w = r^2$; if Tails he shows her $w = r^2y$. Now he asks Peggy: "Was my coin Heads or Tails?" If y is not square then Peggy answers infallibly, since w is a square if and only if the coin was Heads. However, if y *is* a square then Peggy cannot tell whether w incorporates y or not and will answer falsely with probability 1/2. Now performing the exchange 20 times will reduce the chance of a consistently false answer to $1/2^{20} \approx 1$ in a million.



r_1	r_2	r_1^2	$r_2^2 y$	coin2
2	7	4	294	H
5	4	25	96	T
1	5	1	150	H
3	2	9	24	H
4	1	16	6	T

*The Small Print

What if Victor tries to exploit Peggy's omniscience? The delicate exchange illustrated above forces Victor to prove he is adhering to the protocol. He produces a series of random pairs (r_1, r_2) and uses them to make 'dummy' w pairs which he shows (the π's) to Peggy, with their order reversed when a tossed coin (coin2) is Tails. Peggy tosses a coin (coin3) and demands further information: **Tails:** she must see (r_1, r_2) and she confirms this pair by checking it contains the square root of one of the π entries; **Heads:** she must see $r_i w/r$ and she confirms this by checking it is a square root of one of the entries of $\pi \times w$. These checks are enough to confirm that w is either r^2 or r^2y but not enough to reveal which one.

Zero-knowledge provability was introduced by Shafi Goldwasser, Silvio Micali and Charles Rackoff in the mid-1980s. Their work was one of the catalysts for a decade of breakthrough results in computability culminating in the celebrated PCP Theorem. They shared the first Gödel Prize in 1993 with Lazlo Babai and Shlomo Moran.

Web link: www.jbledin.com/papers (click on 'Challenging Epistemology')

Further reading: *The Nature of Computation* by Christopher Moore and Stephan Mertens, Oxford University Press, 2011.