Joe Hurd
Trinity College
20 January 1997

TMS 15 minute talk

Blum Integers

Cryptographic Element

Defn: A **Blum integer** n is the product of two primes $n = pq$ with $p, q \equiv 3 \mod 4$.

Theorem: *Suppose we have a quadratic residue* $x \mod n$.
Then x *has four square roots* mod n *and exactly one* y *of these is a quadratic residue* mod n.

Proof: By the Chinese remainder theorem the multiplicative group is $\mathbb{F}_p^* \times \mathbb{F}_q^*$ with multiplication performed like this:

$$(a, b) \cdot (c, d) = (ac, bd)$$

Thus exactly a quarter of all elements are quadratic residues, and they each have exactly 4 square roots of the form $(\pm\alpha, \pm\beta)$.

Since $p, q \equiv 3 \mod 4$ exactly one of $\pm a$ is a quadratic residue in $\mathbb{F}_p^*, \mathbb{F}_q^*$.
Therefore exactly one of $(\pm\alpha, \pm\beta)$ is a quadratic residue. □

Defn: Call this unique root y the **principal square root** of x.

Theorem: *Taking square roots* mod n *is* RP*-equivalent to factoring* n.

Proof: If we can factor $n = pq$ we take our number $x \mod n$, calculate

$$\pm x^{\frac{1}{2}(p-1)} \mod p$$
$$\pm x^{\frac{1}{2}(q-1)} \mod q$$

and obtain all four square roots.

Conversely, if we can take square roots mod n, then we take a random $u \mod n$, and input $u^2 \mod n$ to our square root algorithm.
Since there are four square roots of $u^2 \mod n$, with probability $\frac{1}{2}$ it will output $v \not\equiv \pm u \mod n$.
In this case, we have

$$u^2 \equiv v^2 \mod n \;\Rightarrow\; u^2 - v^2 \equiv 0 \mod n \;\Rightarrow\; (u - v)(u + v) \equiv 0 \mod n$$

and we have factored n. □

Cryptographic Protocol

Bit commitment: Alice and Bob want to toss a coin fairly over a network.
(i): Alice picks a large Blum integer $n = pq$ and a quadratic residue x with principal square root y. She sends n, x to Bob.
(ii): Bob has to guess whether y lies in the range $H = (0, \frac{1}{2}n)$ or the range $T = (\frac{1}{2}n, n)$ when reduced mod n. He picks either H or T and sends it to Alice.
(iii): Alice sends Bob z, p, q where $z^2 \equiv y \mod n$.

There is no possibility for Alice to cheat since Bob can verify everything she has done. The only way for Bob to cheat is to try and calculate y in advance, but this is RP-equivalent to factoring n.

So we now have a protocol where Alice can commit to Bob some information and thereafter she may not change it, but Bob cannot read it without Alice's help.

Cryptographic System

Alice: I know a really good secret.
Bob: No you don't.
Alice: Yes I do.
Bob: Do not!
Alice: Do!
Bob: Prove it!
Alice: Alright, I'll tell you. *She whispers in Bob's ear.*
Bob: That's interesting. Now I know it, too. I'm going to tell the Daily Mirror.
Alice: Oops.

Suppose Alice's secret was a Hamilton cycle in a really huge graph. This problem is NP-complete, so it could really be the solution to an instance of any other NP problem transformed into the Hamilton cycle. This might be a satisfying assignment of a big combinational circuit, the key to Bob's favourite crypto system, or even something interesting.

Alice wants to prove to Bob she has the secret, but without telling him what it is.

Zero-knowledge proof: Alice proves to Bob she has found a Hamilton cycle H in a graph G.
(i): Alice swaps all the vertex labels on G to create graph G'. She then commits to the vertex pairing she used $f : G \to G'$ and the new Hamilton cycle $H' = f(H)$. She sends G' and these commitments to Bob.
(ii): Bob tells Alice whether he wants to see H', a Hamilton cycle in G' or f, which proves G is the same graph as G'.
(iii): Alice gives Bob the key to the one he asked for.
(iv): The protocol repeats for as many steps as Bob likes.

So who can cheat? If Alice does not know H, she can produce G' which is either isomorphic to G or has a Hamilton cycle H', but not both. So sooner or later Bob will catch her. Can Bob deduce the secret? The only way would be for him to request H' and then try and reconstruct the graph isomorphism, but unfortunately this NP-complete problem is just as hard as finding H in the first place.