MATCHMAKING FOR TIMID COMPUTER SCIENTISTS (AND MATHEMATICIANS)

GENE S. KOPP

Yenta thinks Alice and Bob, her two computer scientist friends, would make a perfect couple. The problem is, neither Alice nor Bob has the guts to ask the other out or even indicate affection in any way. It's not that they fear rejection; rather, somewhat like Beatrice and Benedick in *Much Ado About Nothing*, they seek plausible deniability. Alice must not give away information about her true feelings to anyone—even Yenta—should she wish to lie about them later, and similarly for Bob.

So, Yenta proposes a zero risk way for Alice and Bob to determine whether they should be a couple. If both of them want to date, her algorithm will tell them so. If, on the other hand, Alice doesn't like Bob, Alice will be none the wiser as to Bob's feelings, and Bob will maintain plausible deniability. Similarly, if Bob doesn't like Alice. Finally, no matter what, Yenta learns nothing about her friends' feelings.

Oh, two more things. Alice, Bob, and Yenta each has a private fair coin, with sides labeled "0 (mod 2)" and "1 (mod 2)." Also, the three can communicate with one another privately—by whispering, text message, what have you.

Let $a \in \mathbb{Z}/2\mathbb{Z}$ be 1 if Alice wants to date Bob, and 0 otherwise. Similarly, let $b \in \mathbb{Z}/2\mathbb{Z}$ be 1 is Bob wants to date Alice, and 0 otherwise. Alice and Bob should date if and only if $ab = 1$. The algorithm will return the value of ab to both Alice and Bob.

The algorithm runs as follows. Alice flips her coin and calls the result a_1. Then, she chooses a_2 so that $a = a_1 + a_2$ (all arithmetic taking place in $\mathbb{Z}/2\mathbb{Z}$). Already something unusual has happened: The bit a_2 contains no information; you can check that it has a 50/50 chance of being 0/1, no matter what a is. We have split a bit of information, a, as a sum (modulo 2) of individually informationless bits, a_1 and a_2.

Bob does the same thing as Alice, writing his bit $b = b_1 + b_2$ for a random coin flip b_1. Yenta flips her coin as well, and she records the answer as c_1. Events now proceed as follows.

Phase 1: Alice sends a_1 to Bob and a_2 to Yenta. Bob sends b_1 to Alice and b_2 to Yenta.
Phase 2: Yenta writes $a_2b_2 = c_1 + c_2$, then sends c_1 to Alice and c_2 to Bob.
Phase 3: (Reveal Phase) Alice and Bob now share the product ab between them *as a sum*, not just as a product. Specifically,

$$ab = (a_1b_1 + a_2b_1 + c_1) + (a_1b_2 + c_2) = \alpha + \beta. \tag{1}$$

Alice knows the red bit α; Bob knows the blue bit β. So, Alice simply sends α to Bob, and Bob sends β to Alice. Now, they both know ab, and the algorithm is complete.

Did Phase 3 seem sketchy, like Alice and Bob just revealed more information than they should? To confirm that they didn't, think about what they are trying to accomplish: They want to gain knowledge of ab, revealing no other information to one another, and no information whatsoever to Yenta. In other words, they wish to simulate the effect of an omnipotent being simply *telling* each of them ab.

These notes are based on a talk given in 2010 by John D. Wiltshire-Gordon and the author.

Alice starts with some prior probability distribution on Bob's feelings. Maybe she thinks there's a 65% chance he likes her and a 35% chance he doesn't; to be general, say x and $1-x$. Determine how sudden knowledge of ab would change this distribution, and on the other hand how the algorithm would change this distribution. They should be the same. Do a similar check for Bob's and Yenta's priors. (Of course, Yenta is allowed any prior distribution she pleases on the four-point set $\{(0,0),(0,1),(1,0),(1,1)\}$ of possible values for (a,b).)

The timid computer scientist algorithm is the most difficult of the basic cogs needed to build "secret sharing schemes" to perform any secret computation on private data using three or more people. To imagine how this works, first think about how to encode any (finite) computation as a bunch of addition and multiplication modulo 2. Then, try to convert this to a secret sharing scheme.