Secret Sharing With Cards

Douglas Ulrich

November 9, 2015

1 Exchanging secret bits

Consider a card game played on a deck of 9 cards (cards 1 through 9); Alice and Bob will be on one team, Eve will oppose them. Each player is dealt 3 cards at random; the goal of the game is for Alice and Bob to secretly decide upon a bit (1 or 0) using only public communication.

The strategy for Alice and Bob is as follows:

First, Alice picks at random one card in her hand, x, and one card not in her hand, y. She then declares: "I have one of $\{x, y\}$." (She does not indicate which among these she has.)

Then, if Bob has one of $\{x, y\}$, he says "So do I." (This card will necessarily be y.) Then Alice knows Bob has y, and Bob knows Alice has x; but Eve knows neither of these facts. So Alice and Bob will agree upon the bit 0, if $x < y$; and they will agree upon the bit 1 if $y < x$.

On the other hand, if Bob does not have one of $\{x, y\}$, he says so; and Alice says, "Eve has $\{y\}$." In this case, all players know that Alice has x and Eve has y.

Play proceeds now as if Alice no longer had x and Eve no longer had y; i.e. Alice and Eve both have two cards now. Since Bob has more cards then Alice, he is the next person to randomly choose z in his hand and w not in his hand; he then announces "I have one of $\{z, w\}$."

Alice responds as Bob did previously: either she has w or she does not. If she does, then Alice and Bob can again agree upon the bit 0 if $w < z$, and the bit 1 if $z < w$. Otherwise, Bob and Eve both lose a card.

Then Alice declares a pair, and either Alice and Bob find a secret bit or else Alice and Eve lose another card.

So now Eve has no cards, Alice has one card and Bob has two cards. Bob declares a pair, and this time Eve cannot have the other card; so Alice and Bob can agree on a bit at last.

EXAMPLES

Suppose Alice is dealt $\{1, 2, 3\}$, Bob is dealt $\{4, 5, 6\}$, and Eve is dealt $\{7, 8, 9\}$. Here are three possible plays:

Number 1:
Alice: I have one of $\{1, 4\}$.
Bob: So do I.
Conclusion: They agree on the bit 0, since $1 < 4$ and Alice has 1.

Number 2:
Alice: I have one of $\{1, 7\}$.
Bob: I don't.
Alice: Eve has 7.
Thus Alice currently has $\{2, 3\}$, Bob has $\{4, 5, 6\}$ and Eve has $\{8, 9\}$.
Bob: I have one of $\{4, 2\}$.
Alice: So do I.
Conclusion: They agree on the bit 0, since $2 < 4$ and Alice has 2.

Number 3:
Alice: I have one of $\{1, 7\}$.
Bob: I don't.
Alice: Eve has 7.
Then Alice currently has $\{2, 3\}$, Bob has $\{4, 5, 6\}$ and Eve has $\{8, 9\}$.
Bob: I have one of $\{4, 8\}$.
Alice: I don't.
Bob: Eve has 8.
Thus Alice currently has $\{2, 3\}$, Bob has $\{5, 6\}$, and Eve has $\{9\}$.
Alice: I have one of $\{2, 9\}$.
Bob: I don't.
Alice: Eve has 9.
Now Alice has $\{3\}$, Bob has $\{5, 6\}$ and Eve has nothing. Thus Alice and Bob know each other's hands, but Eve does not.
Bob: I have one of $\{5, 3\}$.
Alice: So do I. (Although you knew that.)
Conclusion: They agree on the bit 0, since $3 < 5$ and Alice has 3.

2 What if Eve has no cards?

It may be the case that after a while Eve has no cards. This sounds like its a good thing, and it is, but how many bits can Alice and Bob then exchange.
Example: Alice has $\{1, 3\}$, Bob has $\{2, 4\}$, and Eve has nothing. So Alice and Bob know all about the cards and who has what. But how can they use this to exchange bits.

With 4 cards: Alice has 2, Bob has 2, how many possibilities would that be? Or, what does Eve know? Eve knows that ONE of the following is true:

Alice	Bob
$\{1,2\}$	$\{3,4\}$
$\{1,3\}$	$\{2,4\}$
$\{1,4\}$	$\{2,3\}$
$\{2,3\}$	$\{1,4\}$
$\{2,4\}$	$\{1,3\}$
$\{3,4\}$	$\{1,2\}$

These are SIX possibilites. Lets call them $C_1, C_2, C_3, C_4, C_5, C_6$.

Alice yells out FOUR of the configurations, ONE Of which is the correct one. For example, he could yell out

$$C_6, C_3, C_2, C_4$$

(THINK of this as the 0th, 1st, 2nd, 3rd)

NOTE that the SECOND one is the correct one, so they have just exchanged the number 2 or, in binary 10.

More generally, if there are A possibilities, let a be the highest power of 2 that is $\leq A$. Alice and Bob will share a number in $\{0, 1, 2, \ldots, a-1\}$. Alice will yell out a of the C_i in some random order except that the CORRECT one is in position p and p is shared secret string of bits.

3 The Complete Protocol

We now give the complete protocol and try to maximize the number of bits.

Convention: If Alice and Bob share a pair then if Alice has the high card the secret bit they share is 1; if Bob has the high card then the secred bit they share is 0.

1. Alice has a cards, Bob has b cards, Eve has c cards. If $a = 0$ or $b = 0$ then STOP.
2. If $a, b, e \geq 1$ then do the following
   (a) Assume that $a \geq b$ (if not then reverse the roles of Alice and Bob). Alice picks a random card x in her hand and a random card y not in her hand. Alice yells out either x, y or y, x (flip a coin to decide).
   (b) Bob looks at his cards.
   Case 1: If one of them is in his hand then he says I HAVE ONE OF THOSE CARDS. They now share a secret bit (use our convention). Alice and Bob put the cards in the pair down. GOTO step 1, but note that Alice has one less card, Bob has one less card, and Eve has the same number of cards.
   Case 2: If none of them is in his hand then he says I DO NOT HAVE EITHER OF THOSE CARDS. Alice now knows that Eve has y. So Alice says I HAVE x AND EVE HAS y. Those cards are now out of the game. GOTO step 1, but note that Alice has one less card, Bob has the same number of cards, Eve has one less card.

(c) If $e = 0$ then let $P = \binom{(a+b)!}{a!b!}$ Let $s = \lfloor \log_2 P \rfloor$. Note that 2^s is the largest power of 2 that is $\leq P$. Ahead of time $C_1, \ldots, C_P$ be the set of all P ways the cards can be distributed to Alice and Bob. (Note that $C_1, \ldots, C_P$ are known to Alice, Bob, and Eve.) Let C_i be the actual configuration that Alice and Bob have (Note that only Alice and Bob know C_i.)

Alice picks 2^s random numbers, though he MUST include i. Alice broadcasts this set in some order. Think of these numbers as being the 0th, 1st, 2nd,..., $(2^s - 1)$nd numbers. (Write those numbers in binary.) Alice and Bob know which of these numbers is the real i. The secret they share is the PLACE it is in.

EXAMPLE: $a = 4$, $b = 2$, $P = \binom{6!}{2!4!} = 15$. So $s = 3$.

Say Alice and Bob have Configuration C_{11}.

Alice will output 8 numbers in $\{1, \ldots, 15\}$ but one of them must be 11.

For educational value we also list the place the number is in in binary.

000	001	010	011	100	101	110	111
8	3	14	1	11	5	9	10

Since 11 is in the 100 place, the shared secret is 100.

NOTE- in this case we DO NOT GOTO step 1. We are DONE.