Secret Sharing With Cards
Bill Gasarch and Douglas Ulrich

1 Introduction

The Diffie-Helman key exchange is believed to be *computationally secure* meaning that we think Eve cannot crack the code in *reasonable time*. Is there a protocol such that Alice and Bob can be guaranteed *information theoretic security*. That is, even if Eve has unlimited computing power she cannot find the key.

We have seen on example of this before- the 1-time pad. That used True Randomness. However, in that scenario Alice and Bob still need to meet. Here we give a key-exchange that is informationally secure and Alice and Bob do not have to meet. Sounds great yes? Not really- this is more of a fun-game thing. My friends in finance tell me that it could never be used. My friends who play bridge (and I do have some) tell me that a bridge bidding scheme based on these concepts was BANNED from tournament play. Peter Winkler, who devised that scheme, is delighted- it's proof that the scheme really worked.

2 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.

3 Generalize

There are n cards labeled $1, 2, 3, \ldots, n$. Alice gets a cards, Bob gets b cards, Eve gets e cards.
PROT(a, b, e) We do the case where $a \leq b$. The case where $a > b$ is similar.

1. If $e = 0$ then Alice and Bob KNOW each others hands. We consider this later; however, the number of bits they can exchange is $\log_2(\binom{(a+b)!}{a!b!})$.

2. Bob picks a card in his hand and a card not in his hand at random. Call them x (in his hand) and y (not in his hand). Bob flips a coin to decide if he will say (x, y) or (y, x). We'll assume its (x, y).

3. Bob YELLS *I HAVE ONE OF* x, y *IN MY HAND* (or "y, x" if that's how the coin flip went)

   (a) If Alice has one of $\{x, y\}$ then Alice says I HAVE ONE OF THOSE ALSO! If Alice has the LOWER of x, y then the shared secret it is 0. If Alice has the HIGHER of x, y then the shared secret it is 0. Alice and Bob put the card aside and then do PROT$(a-1, b-1, e)$.

   (b) If Alice has NONE of $\{x, y\}$ then Alice says *I HAVE NONE OF THEM.* Then Bob will say *I HAVE* x*, EVE MUST HAVE* y. Bob discards x. Eve will then discard y in disgust. (even if she doesn't do it literally Alice and Bob KNOW that she has it so its effectively gone.) NO bits are shared; however, Alice and Bob now do PROT$(a, b-1, e-1)$.

4 The $e = 0$ Case

In the case of $e = 0$ Alice and Bob KNOW each others hands. There are $\binom{(a+b)!}{a!b!}$ total hands. IF this was a power of two THEN they could (ahead of time) agree to list all possible hands lexicograhically and agree that if they have hand H_i they use bit sequence i. This would be $\log_2(\binom{(a+b)!}{a!b!})$ shared secret bits.

Alas, $\binom{(a+b)!}{a!b!}$ is NEVER a power of two. However, we can still use this kind of reasonsing. Let 2^m be the power of 2 that is JUST below $\binom{(a+b)!}{a!b!}$. Note that $m = \log_2(\binom{(a+b)!}{a!b!})$.

1. Alice looks at her cards. She knows Bob cards. Let H be the hand (so H is (ALICES CARDS, BOBS CARDS).

2. Alice picks AT RANDOM $2^m - 1$ hands (none her own). Alice takes those hands, and her own, and RANDOMLY orders them. She says the 2^m hands out loud in that order. We THINK of them as being (if $m = 3$) Hand 000, Hand 001, Hand 010, Hand 011, Hand 100, Hand 101, Hand 110, Hand 111. NOTE that ONE of these is (Alice cards, bobs cards) ALICE knows which that is. (In our example its indexed by three bits: $H_{b_0 b_1 b_2}$).

3. Bob also knows which one of these is (Alice's cards, Bob's cards). So Alice and Bob both know the sequence of bits. THAT is the shared secret key.