Secret Bit Transmission Using a Deck of Cards

Brent Dorman

December 18, 2007

1 Introduction

Alice, perhaps a spy or dishonest bridge player, wishes to transmit a single bit s' secretly to Bob. To ensure secrecy Alice does so by using a one-time pad, in this case, one bit long. A shared secret bit s must first be established with both Alice and Bob. Using s, Alice calculates $q = s \oplus s'$ and sends the value to Bob, who then retrieves $s' = q \oplus s$. Of course, Alice and Bob must first establish the bit s.

We will begin by presenting a protocol for the transmission of one bit. We will then extend this protocol to establish a multiple bit secret.

1.1 Assumptions

As always, assume that there is a malevolent third party Eve. Eve is trying to discover s. We assume Eve has knowledge of whatever protocol Alice and Bob are using, she has infinite computing power, and that she can hear everything said between Alice and Bob. Therefore it is essential that whatever protocol Alice and Bob use allows them to establish the bit s while providing no information to Eve. It is not good enough that it is only unlikely Eve discover s, after all she has infinite computing power, but it must be impossible that she can do better than simply guess.

1.2 A Deal of Cards

The shared secret bit s will be established through the use of a deck of n unique, ordered cards. Each of Alice, Bob, and Eve will be dealt a hand.

> A random deal of cards is an ordered pair (a, b, e) where, out of the deck, Alice is dealt a cards, Bob is dealt b cards, and Eve is dealt $e = n - (a + b)$ cards. Each player only knows the cards held in their own hands. However, a, b, e, and n are all public information.

Under set parameters a *random deal* of cards can be used to establish a shared secret bit s between Alice and Bob.

2 A Randomized Algorithm

A random deal of cards (a, b, e) can be used to establish a secret bit s between Alice and Bob.[1]

2.1 Definitions

> A *pair* $p = (x, y)$ consists of two cards from the *random deal*, x and y. One of them is held by Alice and the other by Bob.

Assume Alice holds the card x in her hand and Bob holds the card y. If Alice and Bob both know the pair $p = (x, y)$ exists, they therefore know who holds which card by a simple process of elimination. Eve, however, even if she knows the pair p exists, cannot tell which card Alice holds and which one Bob holds. The best she can do is guess at who holds what.

2.2 Use p to Establish s

Assume that Alice and Bob can establish a pair $p = (x, y)$. In doing so they know who holds x and who holds y. Recall that x and y come from a deck of unique, ordered cards, so we can establish an operator to determine if $x < y$ or if $x > y$. We will have Alice and Bob agree beforehand that if Alice holds the lesser of the two cards, $s = 1$ and if Alice holds the larger card $s = 0$.

Once the pair p is established Alice and Bob can therefore determine s. Eve, however, has no knowledge of who holds what card, so she cannot determine s. The value s will be Alice and Bob's one time pad.

2.3 Establishing a Pair

Alice and Bob can establish a pair p. Begin with a random deal (a, b, e) $a \geq 1, b \geq 1, e \geq 0$ from the deck and proceed as follows:

1. For simplicity, and without loss of generalization, call whichever player who holds the most cards Alice and the other player Bob. Therefore, in all cases $a \geq b$.

2. Alice selects a card x in her hand and a card y not in her hand to try to create a pair p. She then announces the pair, either $p = (x, y)$ or $p = (y, x)$, to everyone. She will randomly choose which of these two pairs to announce. This ensures that Eve cannot determine who holds what by the order in which x and y are announced in the pair.

3. If Bob holds y he says that p is a valid pair. Now Alice and Bob have established a pair between them and establish s.

4. If Bob does not hold y say that p is not a valid pair. Alice announces the locations of the cards x and y to all, namely that she holds x and Eve holds y. These cards are then discarded from the deck, and the protocol starts over with a new random deal $(a - 1, b, e - 1)$.

The protocol ends when either $a = 0$ or $b = 0$.

2.4 Bounds On Single Bit Transmission

Theorem 1:

> Alice and Bob can establish a shared secret bit s from a random deal (a, b, e) of a deck of n cards so longs as $a \geq 1$, $b \geq 1$, and $a + b \geq e + 2$.

Proof:

> We will proceed by induction on $(a + b)$.
>
> *Base Case:* Since $a + b = 2$ and $a \geq 1, b\ geq 1$ we take $a = 1$, $b = 1$, and $e = 0$. So $a + b = 2 \geq e + 2 = 2$.
>
> Running through the protocol in this case, Alice and Bob establish a pair p on the first run through no matter what because $e = 0$.

Induction: Assume a pair p can be established for the random deal (a, b, e) when $a \geq 1$, $b \geq 1$, and $a+b \geq e+2$. We will induct on $(a+b) \longrightarrow (a+b)+1$

1. If e remains constant we run the protocol. If Alice and Bob exchange a bit, we're done. Otherwise Alice loses a card. This reduces the $(a+b)+1$ case to the $(a+b)$ case, which we assume works by our hypothesis.
2. However when a and b gain an additional card e can also gain a card. The bounds still hold since $(a+b)+1 \geq (e+1)+2$ is clearly true if $(a+b) \geq e+2$. Going through one pass of the protocol, one of two things happens:
   (a) The protocol works out successfully, Alice and Bob establish a pair p.
   (b) The pair p consists of one card held by Alice and another by Eve. These two cards are "outed" and the procedure begins anew with the random deal $(a-1, b, e-1)$. Substituting these values into our initial conditions we find that $((a-1)+b)+1 \geq ((e-1)+1)+2 \longrightarrow (a+b) \geq e+2$. This case holds by our hypothesis! Therefore, Alice and Bob are guaranteed to establish a pair p.

We have proven a base case and that if we can establish pair when Alice and Bob's joint hand size if $(a+b)$, they can also establish a pair when their joint hand size if $(a+b)+1$. Proceeding by induction we find that Alice and Bob are indeed guaranteed a pair for all values a, b, and e so long as $a \geq 1$, $b \geq 1$, and $a+b \geq e+2$.

End Of Proof

3 Establishing Multiple Bits

To transmit multiple bits Alice and Bob use several repeated rounds of the one bit procedure. Rather than stopping after successfully establishing a valid pair, and subsequently getting a shared bit, Alice and Bob discard both cards $x, y \in p$. Now the protocol repeats with a new random deal $(a-1, b-1, e)$.

This continues, with Alice and Bob either establishing shared bits or outing one of Eve's cards each round, until either $a = 0$ or $b = 0$.

3.1 Bounds on Multiple Bits

Theorem 2:

A $(a, b, 0), a \geq b \geq 1$ random deal guarantees a total of at least b shared bits established.

Proof:

Since Eve holds no cards, Alice and Bob can successfully establish a pair with every pass through the protocol. The $(a, b, 0)$ case reduces to $(a - 1, b - 1, 0) + 1$. This repeats a total of b times, until $b = 0$, so b bits are established in all.

End Of Proof

Theorem 3:

A $(a, b, e), a \geq b \geq 1, a + b \geq e + 2$ random deal guarantees at least $b - \lceil (e - a + b)/2 \rceil$ shared bits established.

Proof:

We are looking for the minimum number of shared secret bits we can guarantee will be established. We must therefore assume that Alice and Bob fail to establish a valid pair every time failure is possible.

Alice and Bob attempt to establish a pair, which fails if Eve holds any cards. Thus $(a, b, e) \longrightarrow (a - 1, b, e - 1)$. Alice and Eve will continue to lose cards until either $a = b$ or $e = 0$. If $e = 0$ before $a = b$, then we apply the formula for the $(a, b, 0)$ case, which was previously proven. Otherwise we continue with a $(a, a, e - (a - b))$ random deal. Set $e' = e - (a - b)$

Alice will announce a possible pair, which we assume fails if Eve holds any cards. Thus $(a, a, e') \longrightarrow (a - 1, a, e' - 1)$. If Eve now holds no cards we are in the previously proven $(a, b, 0)$ case, and $b = a - 1$ bits can be established.

Otherwise, Alice and Bob go through another iteration of the protocol. Again assume they cannot establish a valid pair. Therefore $(a-1, a, e'-1) \longrightarrow (a-1, a-1, e'-2)$. If Eve now holds no cards, Alice and Bob can establish $a-1$ shared bits. If Eve does hold cards call $a' = a-1$ and $e'' = e'-1 = e-2$ so $(a-1, a-1, e-2) = (c', c', e'')$ and we proceed recursively.

For a deal starting when $a = b$ we see that if Eve holds one card, Alice and Bob are guaranteed one less bit. Similarly, two less are guaranteed for three cards, three less for five cards, etc. This can be expressed as $\lceil e/2 \rceil$. Therefore in a (a, a, e) deal, Alice and Bob are guaranteed $a - \lceil e/2 \rceil$ bits.

Recall that to get down from a (a, b, e) deal to a (b, b, e') deal we must run $(a-b)$ rounds of the protocol. Substituting these values into the formula for the (a, a, e) case yields $(b - \lceil e'/2 \rceil) \longrightarrow (b - \lceil (e-a+b)/2 \rceil)$ bits guaranteed to be shared.

End Of Proof

4 A Deterministic Algorithm

A deterministic (Non-random) protocol also exists for Alice and Bob to exchange a secret bit.[1]

4.1 Single Bit Protocol

This protocol works similarly to the randomized algorithm. Begin with a random deal of cards (a, b, e) that will be used to establish the shared secret s.

1. Assign each of the $n = a + b + e$ cards a unique index 0 through $n-1$.

2. If $e = 0$ and both $a \geq 0$ and $b \geq 0$ then we are finished. Alice and Bob have assigned each of the $\binom{n}{a}$ possible $(a, b, 0)$ deals a unique index. Alice and Bob now can establish a shared secret bit based upon the index.

3. If $e \neq 0$ Alice, Bob, and Eve consider the deck as consisting of $\lfloor n/2 \rfloor$ blocks of two cards each. So card $2m$ is in block m rank 0 and card $2m+1$ is in block m rank 1. If n is odd discard card $n-1$.

   > For example, in a deck of $n = 6$ cards the three blocks are $(1, 2)$, $(3, 4)$, and $(5, 6)$.

4. For each block m from 0 through $\lfloor n/2 \rfloor$, Alice and Bob each announce whether or not they hold one of the cards belonging to block m, that is, they hold either card $2m$ or $2m+1$ but not both.
   If both Alice and Bob hold one card belonging to block m they have established a pair and can compute a shared secret bit. Otherwise they know that Eve holds the other card of block m. They repeat this procedure of announcing block for each singleton set in their hand.

5. If Alice and Bob cannot establish a pair they establish a new random deal (a', b', e'). Each of Alice, Bob, and Eve discards all cards belonging to a block m if they hold only one card of that block. If Alice, Bob, or Eve hold both cards of a block m, they discard the rank 1 card of that block.

6. If $a' = 0$ or $b' = 0$ the protocol fails. Otherwise apply it recursively on the new random deal (a', b', e').

4.2 Exchanging Multiple Bits

As with the randomized protocol, enabling the exchange of multiple bits using the deterministic protocol requires some small changes.

1. Assign each of the $n = a + b + e$ cards a unique index 0 through $n - 1$.

2. As in the single bit protocol, consider the deck as consisting of two card blocks. If n is odd discard card $n - 1$.

3. For each block m from 0 through $\lfloor n/2 \rfloor$, Alice and Bob each announce whether or not they hold only one of the cards belonging to the block m.

4. If both Alice and Bob hold one card belonging to block m they have established a pair and can compute one shared secret bit as in the

randomized algorithm. They discard both cards; otherwise they know that Eve holds the other card of block m and instead either Alice or Bob (Whomever holds the card) and Eve discard a card. They continue trying to establish further bits using the remaining blocks of the deal.

5. If $a' = 0$ or $b' = 0$ the protocol ends. Alice and Bob now establish a new random deal (a', b', e'). Each of Alice, Bob, and Eve discards all cards belonging to a block m if they have only one card of that block. If Alice, Bob, or Eve hold both cards of a block they discard the rank 1 card. Apply the protocol recursively on the new random deal (a', b', e')

The primary change in the multiple bit version is that the $e = 0$ case no longer exists.

4.3 Bounds

Theorem 6:

In a $(a, b, 0)$ random deal, Alice and Bob can be guaranteed to exchange a number of bits described by the recursive function $f(a, b)$.
$f(a, 0) = f(0, b) = 0$
$f(a, b) = f(a/2, b/2)$ if a and b are even.
$f(a, b) = f(a/2, (b-1)/2+1)$ if a even and b odd.
$f(a, b) = f((a-1)/2+1, b/2)$ if a odd and b even.
$f(a, b) = f((a-1)/2, (b-1)/2)+1$ if a and b are odd.

Proof:

As with the other proofs, we are looking for a guarantee on the number of bits exchanged. We therefore must assume a worst case scenario. This happens when Alice and Bob hold the maximum number of full blocks in their hand, that is, all cards they hold are in blocks. None of these cards they hold will allow them to establish a bit since no pairs can be established.

The $f(a, 0) = f(b, 0) = 0$ case is obviously true since if either Alice or Bob hold no cards there's no way for them to establish a pair.

The a and b are even case. If both players hold an even amount of cards the worst situation is that they all form full "blocks." Alice and Bob can exchange no bits and both must discard half of their cards before proceeding onto another round.

The one of a or b is even and the other is odd case. Without loss of generality, assume a is even and b is odd. Again in the worst case Alice hand consists of only full blocks, with Bob's hand consisting of all full blocks and one lone card. Since both of them do not hold a "lone" card they cannot establish a pair. Alice discards half of her cards, and Bob, ignoring the lone card, discard half of his and then add's the odd-one-out back in.

The a and b are odd case. If both Alice and Bob hold an odd amount of cards, they have at least one card a piece that doesn't belong to a block. Since Eve has no cards, this means that Alice and Bob each have one card of the same block and can therefore exchange a bit. Any further "lone" cards they hold also allow them to exchange bits, so we assume that rest of their (even) number of cards consist of only blocks. So through losing the one odd-card-out each they exchange one bit, and then discard half of their remaining cards."

4.4 Bounds: Case Studies

Here we will examine some interesting cases of the deterministic protocol.

4.4.1 A Poor Case

The random deal $(2^n, 2^n, 0)$ $n \geq 0$ only guarantees Alice and Bob share one bit, no matter how large their hands are. In the worst case, Alice holds cards 0 through $(n/2) - 1$ and Bob holds cards $(n/2)$ through $n - 1$.

Alice and Bob's hands both consist of only whole blocks. After the first round, half of each of their hands are discarded. However, since they held sequential cards, once again their hands only consists of whole block. They lost half their hands again and again, and eventually get down to a $(1, 1, 0)$ deal. Here they are only able to share 1 bit.

4.4.2 An Ideal Case

Consider the random deal $(2^n - 1, 2^n - 1, 0)$ $n \geq 1$. Here Alice and Bob are guaranteed to share n bits.

In the worst possible case, Alice and Bob each hold full blocks of cards with one left over. They use this one "left-over" card they each hold to establish one shared bit. Since the cards they now hold are all in blocks, their remaining hards are cut in half.

A hand of size $2^n - 1$ is therefore reduced to one of size $2^n - 2$ after establishing the bit, and further reduces to $(2^n - 2)/2 \longrightarrow 2^{n-1} - 1$. This recursion continues until neither Alice nor Bob hold any cards.

With each iteration they can share 1 bit, and thus at the end of the rounds share a total of n bits.

References

[1] M. Fisher, M. Patterson, and C. Rackoff. Secret bit transmission using a random deal of cards. In J. Feigenbaum and M. Merritt, editors, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science: Distributed Computing and Cryptography*, volume 2. The American Mathematical Society, 1991.