Key Exchange with Cards: Generating Extra Bits in Expectation

Thomas DuBois*

Abstract

One of the cornerstones of modern cryptography is the ability for trusted parties to establish a sequence of bits known only to themselves. Using that sequence of bits, they are able to send messages over an insecure channel, and an eavesdropper who does not know the secret bits cannot tell the difference between a legitimate message and a random one. In this paper we analyze an existing randomized protocol for establishing a secret key from a random deal of cards. Worst case bounds are known for the number of bits established using this protocol, however until now no probabilistic analysis has been applied. We show that in expectation and with high probability the protocol will do considerably better in some of the most natural situations than the worst case bounds. We present bounds on the expected number of bits as well as bounds on the probability of large deviation from the expected value. Furthermore, in many of these situations we give upper and lower bounds that approach each other in the limit.

1 Introduction

The ability to send information securely over an insecure channel is at the very heart of cryptography. To achieve this goal, many cryptographic protocols rely upon the establishment of a secret key, which is a bit string known only by those who should have access to the information sent over the channel. In this paper we analyze a model where all parties are dealt a set of distinct cards from a known deck, and then two parties wishing to communicate in secret use their deals and an insecure channel to establish a key. The problem of establishing a secret key using a deal of cards may seem like an unrealistically contrived model. However this problem is a case of the broader and more applicable problem of establishing a key based on a shared source of correlated randomness, which is studied by Maurer and Wolf [MW03]. The protocol we use is initially proposed by Fischer et al. [FPR91]. Though the idea of using a deal of cards to establish a secret key has some foundations in Winkler's work on cryptography and the game of bridge [Win83]. Later, Fischer and Wright refine the work around the protocol we use [FW93, FW96]. Collectively these works give worst case bounds on the number of bits established using the protocol. Additionally they give sufficient conditions on the deck size and the size of the deals for any protocol to guarantee a bit. More recent work establishes necessary and sufficient conditions [KMN08]. However only the cases where at least one bit can be guaranteed are studied. We extend this work to include an analysis of how many bits are established in expectation and with high probability.

Our analysis uses the following protocol:

THE PROTOCOL

*Dept. of Computer Science, University of Maryland, College Park, MD 20742. Supported in part by NSF ITR Award CNS-0426683 and NSF Award CNS-0626964. tdubois@cs.umd.edu. This paper has been submitted for inclusion in the 12th Intl. Workshop on Randomization and Computation.

A deck of n distinct cards (labeled 1 through n) is dealt to three or more parties, Alice, Bob, and their adversaries. Alice and Bob each know only their hand, while we assume that the adversaries are computationally unbounded and can collude. We refer collectively to all adversarial parties as Eve. Alice and Bob wish to establish some secret bits over an insecure channel using the cards in their hands. The key exchange proceeds in rounds. In every round, whomsoever of Alice and Bob has the most cards goes next (ties are broken arbitrarily). The player going first will change frequently throughout the protocol, however we assume without loss of generality that Alice is going next, and we use this naming convention throughout the paper. Alice picks one of her cards x, one card that she does not have y, and a potential key bit all uniformly at random. If her bit is a 0, she sends (x, y) over the channel, if the bit is a 1 she sends (y, x). If Bob has y, he knows the bit and sends an acknowledgment over the channel. At this point they can use the potential key bit and we refer to this round as a hit. Eve knows the pair sent over the channel, and that a bit was established, but she has no way of knowing which of the two cards belongs to Alice and which to Bob. Therefore she cannot determine the bit. If Bob does not have y, then Eve must have it. In this case Bob sends a negative acknowledgment over the channel and they do not establish a key bit this round. We refer to a round where no bit is established as a miss. x and y are both removed from the set of active cards that Alice can use in future rounds.

END OF PROTOCOL

To give this protocol a concrete and natural setting, consider a deck of n cards, dealt evenly or uniformly at random to each of $m \ll n$ players (including Alice and Bob). If the cards are dealt randomly then with high probability (a_0, b_0, e_0) will be very close to $(\frac{n}{m}, \frac{n}{m}, \frac{n(m-2)}{m})$. Either way we can write the initial configuration as approximately $(k, k, (m-2)k)$ with $k = \frac{n}{m}$. In the case of three players we have a (k, k, k) initial configuration. The worst case bounds show that at least $\lfloor \frac{k}{2} \rfloor$ bits will be established and our bounds show that we expect at least $\frac{k}{224}$ extra bits for a total of $\lfloor \frac{k}{2} \rfloor + \frac{k}{224}$. In the case of more than three players, the worst case has no bits being established. In these cases we show that in expectation and with high probability $\Theta(\frac{k}{m-2})$ bits will be established. For example, when there are four players, we improve on the previously known zero bits guaranteed by showing that in expectation at least $\frac{k}{9} = \frac{n}{36}$ bits will be established. Figure (1) shows our upper and lower bounds for a few values of m.

Number of Players m	3	4	5	12	102	1002
$f(k)$ in $(k, k, kf(k))$	1	2	3	10	100	1000
Minimum Guaranteed Bits	k	0	0	0	0	0
Expectation Lower Bound	$k/224$	$k/9$	$k/12$	$k/30$	$k/120$	$k/1017$
Expectation Upper Bound	$k/3$	$2k/3$	$k/2$	$k/5$	$k/98$	$k/998$

Figure 1: This table shows the values for the function f, the minimum number of bits established, and our bounds on the expected number of extra bits established given km total cards dealt evenly to m players.

Our analysis starts with the observation that the protocol describes a Markov process. If we let a_i, b_i, e_i be the number of cards in each of Alice, Bob, and Eve's hands respectively at the start of round i, then at every round i only the current values for a_i, b_i, e_i affect the probability p_i of getting a secret bit during that round. Let X_i denote the event that round i is a hit. Assuming $a_i \geq b_i$, the probability of getting a bit during the i^{th} round is the probability that Alice picks y from Bob's hand, or $p_i = \frac{b_i}{e_i + b_i}$, and that probability decreases for each bit

established. It is known that in a system where Alice, Bob, and Eve initially have a_0, b_0, e_0 cards, at least $\lfloor \frac{a_0+b_0-e_0}{2} \rfloor$ secret bits will be established.

While $\lfloor \frac{a_0+b_0-e_0}{2} \rfloor$ is a tight lower bound on the guaranteed number of bits established, some extra bits are possible. In fact, up to $\min(a_0, b_0)$ bits are possible. This gap between the upper and lower bounds on the number of bits established is significant, particularly when the lower bound is 0. For example, when $(a_0, b_0, e_0) = (k, k, 2k)$ the lower bound is 0 while the upper bound is k. Our contribution in this paper consists of probabilistic bounds on how many extra key bits are established given an initial deal of the form $(a_0, b_0, e_0) = (k, k, k \cdot f(k))$ for a range of functions f. We show bounds on both the expected number of extra bits and the probability of large deviation from the expected value. The probability change from one round to the next is highly dependent on the event X_i. Our main technique to remove this dependency involves creating another sequence of random variables, one for each round in the protocol. We create this sequence such that for any round, the probability of a hit in this sequence is at least (or most) that of the protocol's. We can then apply Chernoff bounds [Che52] to this new sequence which will give a lower (or upper) bound as well as tail bounds on the protocol's expected number of hits.

We decompose the question of how many extra bits are expected into two natural cases,

- How many extra bits are established if none are guaranteed ($f(k) \geq 2$)?
- How many extra bits are established if some are guaranteed ($f(k) < 2$ with $k \cdot \frac{2-f(k)}{2}$ bits guaranteed)?

We address the case where no bits are guaranteed in Section 2. The results are primarily inspired by two observations. First, since the number of guaranteed bits is zero, the number of extra bits is exactly the number of total bits. Thus once a bit is established, it can be added to our count immediately. Second, p_i decreases from one round to the next regardless of whether or not a bit is established. An interesting exception is when $f(k) = 2$. In this case as long as no bits have been established, p_i will stay constant at $\frac{1}{3}$ in each pair of rounds. We use the fact that p_i is non-increasing after each pair of rounds, and bounds on how much it decreases, to create a sequence which stochastically dominates the events X_i. We show that for all values of $f(k) \geq 2$, the expected number of bits is between $\frac{k}{3(1+f(k))}$ and $\frac{2k}{1+f(k)}$. This is significant because no bits are guaranteed, and yet with high probability $\Theta(\frac{k}{1+f(k)})$ are established in practice. Furthermore we use the observation that when $f(k)$ is high, hits are rare, to show that higher values of $f(k)$ will have expected values that quickly approach $\frac{k}{f(k)}$ with deviation bounds given by Chernoff.

In Section 3 we address the case where there are guaranteed bits. This case involves the relative, not absolute, number of bits established because an established bit is not necessarily an extra bit. For similar reasons, p_i may fluctuate up and down as the algorithm progresses. Establishing a bit will lower p and missing will increase p. In this case we establish an upper bound of $\frac{kf(k)}{3}$ on the expected number of bits. Whenever $f(k) \geq 1$ we establish a lower bound of $\frac{k(f(k)-1)}{9}$. Both of these bounds provide a smooth transition from the no guaranteed bits case at $f(k) = 2$. Unfortunately we have no good lower bounds for when $f(k) \ll 1$. We do not view this as significant though since in these cases there are $k \cdot \frac{2-f(k)}{2} \approx k$ guaranteed bits which is much larger than the at most $k \cdot \frac{f(k)}{3}$ extra expected bits.

2 The Case when No Bits Guaranteed

The first case we consider in detail is when no bits are guaranteed, which means $f(k) \geq 2$. Our first step is to upper bound the rate of decrease per round of the hit probability. This allows us to create a sequence which stochastically dominates from below the events X_i. We use this sequence and a trivial upper bound to show that the expected number of extra bits is $\Theta(\frac{k}{f(k)+1})$. Furthermore, for even constant functions $f(k)$, as $f(k) \geq c$ increases above 2, with high probability the number of hits becomes at most a small fraction of the number of rounds. We use this observation to tighten our dominating sequence on both the upper and lower bound. We show that when $f(k) \geq c$, the expectation quickly approaches $\frac{k}{c}$ with upper and lower tail bounds given by Chernoff.

2.1 Lower Bound on the Expectation

Letting $m_i = \min(a_i, b_i)$, the probability of getting a bit in round i is the number of cards in Bob's hand divided by the number of cards in Bob and Eve's hands combined or

$$p_i = \frac{m_i}{e_i + m_i} \tag{1}$$

Once again, Eve may be several adversaries working together. Initially this probability is $\frac{k}{f(k)k+k} = \frac{1}{f(k)+1}$. Since at all steps in the protocol $e_i - e_{i+1} \leq a_i - a_{i+1} + b_i - b_{i+1}$, we inductively have that, for all rounds i, $e_0 - e_i \leq a_0 - a_i + b_0 - b_i$ and thus $e_i \geq (e_0 - a_0 - b_0) + (a_i + b_i) \geq (f(k) - 2)k + 2m_i$.

There are three cases we consider by which the probability of getting a bit can change from round to round.

1. Alice and Bob get a bit. In this case, $a_{i+1} = a_i - 1$, $b_{i+1} = b_i - 1$, and $e_{i+1} = e_i$. Thus

$$p_i - p_{i+1} = \frac{m_i}{e_i + m_i} - \frac{m_i - 1}{e_i + (m_i - 1)} = \frac{e_i}{(e_i + m_i)(e_i + m_i - 1)} > 0$$

2. Alice and Bob do not get a bit, and m decreases. In this case both m and e decrease by 1 giving

$$p_i - p_{i+1} = \frac{m_i}{e_i + m_i} - \frac{m_i - 1}{(e_i - 1) + (m_i - 1)} = \frac{e_i - m_i}{(e_i + m_i)(e_i + m_i - 2)} \geq 0$$

3. Alice and Bob do not get a bit, and m stays the same. In this case p increases in round $i + 1$.

$$p_i - p_{i+1} = \frac{m_i}{e_i + m_i} - \frac{m_i}{(e_i - 1) + m_i} = \frac{-m_i}{(e_i + m_i)(e_i + m_i - 1)} \leq 0$$

When Alice and Bob initially have the same number of cards, a_i and b_i are always the same or one apart, thus cases two and three always alternate with case one interspersed at any point. This can be seen because case two starts with a_i and b_i the same, so $a_i + b_i$ is even, and it finishes with a_{i+1} and b_{i+1} different so their sum is odd. Case three follows the reverse pattern of case two and case one does not change the parity of $a_i + b_i$. This alternation between cases two and three and the fact that e_i never drops below $2m_i$ gives the following lemma:

Lemma 1 *When no bits are guaranteed, for all i, p_{i+2} is at most p_i*

The most p can decrease in two sequential rounds is when case one happens twice in a row, when both rounds are hits. This gives

$$\begin{aligned} p_i - p_{i+2} &= \frac{m_i}{e_i + m_i} - \frac{m_{i+2}}{e_{i+2} + m_{i+2}} \\ &\leq \frac{m_i}{e_i + m_i} - \frac{m_i - 2}{e_i + m_i - 2} \\ &= \frac{m_i(e_i + m_i - 2) - (e_i + m_i)(m_i - 2)}{(e_i + m_i)(e_i + m_i - 2)} \\ &= \frac{2(e_i + m_i) - 2m_i}{(e_i + m_i)(e_i + m_i - 2)} \\ &= \frac{2e_i}{(e_i + m_i)(e_i + m_i - 2)} \end{aligned} \tag{2}$$

We can similarly establish a lower bound on $p_i - p_{i+2}$ when cases 2 and 3 happen as

$$\begin{aligned} p_i - p_{i+2} &= \frac{m_i}{e_i + m_i} - \frac{m_{i+2}}{e_{i+2} + m_{i+2}} \\ &\geq \frac{m_i}{e_i + m_i} - \frac{m_i - 1}{(e_i - 2) + (m_i - 1)} \\ &= \frac{e_i - 2m_i}{(e_i + m_i)(e_i + m_i - 3)} \end{aligned} \tag{3}$$

Also the most the sum $e+m$ can decrease in two rounds is 3 (with one of e and m decreasing by 1 and the other by 2), so $e_{2i} + m_{2i} \geq e_0 + m_0 - 3i$. Thus in each of the first $\frac{1}{2}k$ rounds (the first $\frac{1}{4}k$ pairs of rounds), $e_i + m_i$ must be at least $k(f(k) + 1) - 3\frac{1}{4}k$. Using this we can upper bound $p_i - p_{i+2}$ for each of these rounds by

$$\begin{aligned} \frac{2e_i}{(e_i + m_i)(e_i + m_i - 2)} &\leq \frac{2e_0}{(f(k)k + k - (\frac{1}{4}k)3)(f(k)k + k - (\frac{1}{4}k)3 - 2)} \\ &= \frac{2e_0}{(f(k) + \frac{1}{4})k((f(k) + \frac{1}{4})k - 2)} \\ &\leq \frac{2f(k)k}{(f(k) + \frac{1}{4})f(k)k^2} \text{ (when } k \geq 8) \\ &\leq \frac{2}{(f(k) + \frac{1}{4})k} \end{aligned} \tag{4}$$

Therefore for the i^{th} pair of rounds (up to the $\frac{k}{4}^{th}$ pair), the probability of getting a bit in each round is at least $p_0 - i \cdot \frac{2}{(f(k)+\frac{1}{4})k}$.

Lemma 2 *The expected number of bits established after the first $\frac{k}{2}$ rounds is at least $\frac{1}{3(f(k)+1)} \cdot k$.*

To prove the lemma, take the linearity of expectation over all of those rounds (summing over the pairs), we get that the expected number of bits established is at least

$$\sum_{i=1}^{\frac{1}{4}k} (E[X_{2i-1}] + E[X_{2i}]) \geq \sum_{i=1}^{\frac{1}{4}k} (2Pr[X_{2i} = 1])$$

$$
\begin{aligned}
&\geq 2\sum_{i=1}^{\frac{1}{4}k}\left(\frac{1}{f(k)+1}-i\cdot\frac{2}{(f(k)+\frac{1}{4})k}\right)\\
&= \frac{k}{2(f(k)+1)}-\frac{4}{(f(k)+\frac{1}{4})k}\cdot\sum_{i=1}^{\frac{1}{4}k}i\\
&= \frac{k}{2(f(k)+1)}-\frac{4}{(f(k)+\frac{1}{4})k}\cdot\frac{\frac{k}{4}(\frac{k}{4}+1)}{2}\\
&= \frac{k}{2(f(k)+1)}-\frac{\frac{k}{4}+1}{2(f(k)+\frac{1}{4})}\\
&\geq \frac{k}{2(f(k)+1)}-\frac{\frac{k}{3}+\frac{4}{3}}{2(f(k)+1)} \text{ using that } f(k)\geq 2\\
&= \frac{\frac{2}{3}k-\frac{4}{3}}{2(f(k)+1)}\\
&= \frac{1-O(\frac{1}{k})}{3(f(k)+1)}\cdot k
\end{aligned}
$$

2.2 Upper Bound on the Expectation

From Eq (1) and Lemma (1) we know that the initial hit probability is $p_0=\frac{m_0}{e_0+m_0}=\frac{1}{f(k)+1}$ and that $p_i\geq p_{i+2}$. Combining those results with $p_1<p_0$ (because $m_1=m_0-1$) gives $\forall i, p_i\leq\frac{1}{f(k)+1}$. Using this fact and taking the linearity of expectation over all rounds gives us an easy first order bound. There are no more than $2k$ trials (one for each of Alice and Bob's cards), and for each the probability of establishing a bit is at most $\frac{1}{1+f(k)}$. Therefore the expected number of bits is bounded above by

$$\frac{2}{1+f(k)}\cdot k \tag{5}$$

Define $B_{f,k}$ to be number of bits established starting with an $(a_0,b_0,e_0)=(k,k,kf(k))$ configuration. Using this definition and direct applications of Lemma (2) and Eq (5) gives

Theorem 1 *If $f(k)\geq 2$, then $\frac{1/3-O(\frac{1}{k})}{1+f(k)}\leq\frac{E[B_{f,k}]}{k}\leq\frac{2}{1+f(k)}$*

Thus $EB_{f,k}=\Theta(\frac{k}{1+f(k)})$. And furthermore, the event that a bit is established in round i is negatively correlated with the sum of the previously established bits (because the change in p is always more negative when a bit is established). Therefore Chernoff like tail bounds apply, and the probability that $B_{f,k}$ deviates by a factor of $\frac{x}{\sqrt{E[B_{f,k}]}}$ is exponentially small in x.

2.3 Tighter Bounds

There is a constant factor gap of 6 between our upper and lower bounds above. In this section we show much tighter bounds when $f(k)=\Omega(1)$ where the hidden constant is even moderately large and $f(k)=O(\frac{k}{\log k})$. We require $f(k)=O(\frac{k}{\log k})$ so that $E[B_{f,k}]=\Omega(\log k)$ which is necessary for Chernoff to give large deviation probabilities on the order of $k^{-\Omega(c)}$. Our analysis relies primarily on bounding the change in probabilities after two steps. From Equations (2 and 3) we know that for all i $\frac{e_i-2m_i}{(e_i+m_i)(e_i+m_i-3)}\leq p_i-p_{i-2}\leq\frac{2e_i}{(e_i+m_i)(e_i+m_i-2)}$.

The upper bound comes from the case where a bit is established, and the lower bound comes from the case where no bits are established. The numerator of the lower bound can be as low as $k(f(k)-2)$. Thus when $f(k)=2$ the lower bound is zero. However as $f(k)\to\infty$ the lower bound approaches $\frac{1}{2}$ the upper bound.

It is useful to observe that if $f(k)$ is small, there is a lot of entropy in the process, for example when $f(k)=2$ the probability of getting a bit starts at $\frac{1}{3}$. However if $f(k)$ is large, we expect that almost all attempts to establish a bit will fail.

For the remainder of this section we will use c in place of $f(k)$ in the analysis. We do this to emphasize that the bounds derived are tight even with $f(k)$ as low as a constant.

Notice that when c is high, we expect the majority (at least $\frac{c}{1+c}$) of the trials not to establish a bit, and therefore only decrease p by the smaller amount. We now upper bound the number of times that p can decrease by more than $\frac{e_i-2m_i}{(e_i+m_i)(e_i+m_i-3)}$ in two rounds. There are at most $2k$ trials, one for each card dealt to Alice and Bob. Each trial i has a bit establish probability $p_i \le \frac{1}{1+c}$. Therefore we can apply Chernoff bounds with $\mu=\frac{2k}{1+c}$ to the upper tail of bits established. Specifically, the probability that $B_{f,k} \ge \frac{2k}{1+c}+\sqrt{3\frac{2k}{1+c}\log k}$ is at most $\frac{1}{k^2}$. Next we bound $E[B_{f,k}]$ by its expectation given at most $\frac{2k}{1+c}+\sqrt{3\frac{2k}{1+c}\log k}$ bits are established.

$$E[B_{f,k}] \;\ge\; E\left[B_{f,k}|B_{f,k}<\frac{2k}{1+c}+\sqrt{3\frac{2k}{1+c}\log k}\right] \tag{6}$$

For any c we can find k_0 such that for $k\ge k_0$ we can bound $\frac{2k}{1+c}+\sqrt{3\frac{2k}{1+c}\log k}\le\frac{3k}{1+c}$.

With probability at least $\frac{k^2-1}{k^2}$, for all but at most $\frac{3k}{1+c}$ values of i, no bits are established in the i^{th} pair of rounds. For this majority of rounds
$p_{2i}-p_{2i+2}=\frac{m_i}{e_i+m_i}-\frac{m_i-1}{e_i+m_i-3}=\frac{e_i-2m_i}{(e_i+m_i)(e_i+m_i-3)}$ and for those (at most $\frac{3k}{1+c}$) values of i where a bit is established $p_i-p_{i+2}\le\frac{m_i}{e_i+m_i}-\frac{m_i-2}{e_i+m_i-2}=\frac{2e_i}{(e_i+m_i)(e_i+m_i-2)}$.

To lower bound the expectation $E[B_{f,k}]$, we first note that given at most $\frac{3k}{1+c}$ bits are established over the course of the protocol, the sum of $2p_{2i}$ over all pairs of rounds i is minimized when all of the bits are established first and all subsequent rounds do not establish any bits. In this case p_i after that initial string of successes is

$$\begin{aligned}
p_{6k/(c+1)} &\ge p_0-\sum_{i=1}^{3k/(c+1)} p_{2i}-p_{2i-2}\\
&\ge \frac{1}{c+1}-\frac{3k}{c+1}\cdot\frac{2e_0}{(e_i+m_i)(e_i+m_i-2)}\\
&\ge \frac{1}{c+1}-\frac{3k}{c+1}\cdot\frac{2kc}{k^2(c-2)^2}\\
&= \frac{1}{c+1}-\frac{6c}{(c+1)(c^2-4c+4)}\\
&= \frac{1-\frac{6}{c-4}}{c+1}
\end{aligned}$$

In this lower bounding scenario, after the initial $6k/(c+1)$ rounds, no more bits are established, and the probability after two rounds is always a decrease by $\frac{e_i-2m_i}{(e_i+m_i)(e_i+m_i-3)}<\frac{(c+1)k}{(c-2)^2k^2}$.

Thus the total expected sum is at least

$$\begin{aligned}
E[B_{k,f}] &\geq E\left[B_{f,k}|B_{f,k} < \frac{2k}{1+c} + \sqrt{3\frac{2k}{1+c}\log k}\right] \text{ from Eq (6)} \\
&= \sum_i \left[p_i|B_{f,k} < \frac{2k}{1+c} + \sqrt{3\frac{2k}{1+c}\log k}\right] \\
&\geq \frac{6k}{(c+1)} \cdot \frac{1-\frac{6}{c-4}}{c+1} + \sum_{i=1}^{2k-3k/(c+1)} \left(\frac{1-\frac{6}{c-4}}{c+1} - \frac{i}{2} \cdot \frac{(c+1)k}{(c-2)^2k^2}\right) \\
&= 2k \cdot \frac{1-\frac{6}{c-4}}{c+1} - \sum_{i=1}^{2k-3k/(c+1)} \left(\frac{i}{2} \cdot \frac{(c+1)}{(c-2)^2k}\right) \\
&= 2k \cdot \frac{1-\frac{6}{c-4}}{c+1} - \frac{(c+1)}{2(c-2)^2k} \cdot \sum_{i=1}^{2k-3k/(c+1)} i \\
&= 2k \cdot \frac{1-\frac{6}{c-4}}{c+1} - \frac{(c+1)}{2(c-2)^2k} \cdot \binom{k\frac{2c-1}{c+1}}{2} \\
&\geq 2k \cdot \frac{1-\frac{6}{c-4}}{c+1} - \frac{4k(c+1)(c-1/2)^2}{4(c+1)^2(c-2)^2} \\
&= \Theta(\frac{k}{c}) \qquad (7)
\end{aligned}$$

We can similarly upper bound $E[B_{k,f}]$ by noticing that the decrease in probability every two rounds is at least $\frac{e_i-2m_i}{(e_i+m_i)(e_i+m_i-3)} > \frac{(c-2)k}{(c+1)^2k^2}$. Therefore

$$\begin{aligned}
E[B_{k,f}] &\leq \sum_{i=1}^{2k} \left(\frac{1}{1+c} - \frac{i}{2} \cdot \frac{(c-2)k}{(c+1)^2k^2}\right) \\
&= \frac{2k}{c+1} - \frac{(c-2)}{2(c+1)^2k} \cdot \sum_{i=1}^{2k} i \\
&= \frac{2k}{c+1} - \frac{(c-2)(2k+1)}{2(c+1)^2} \\
&= \Theta(\frac{k}{c}) \qquad (8)
\end{aligned}$$

Theorem 2 *For any $f(k)$ such that $f(k) \geq c$, as $c \to \infty$ the expectation $E[B_{f,k}]$ approaches $\frac{k}{c}$ with lower error term at most $O\left(\frac{c-1/2}{c-2}\right)^2$ and upper error term at most $O\left(\frac{c-2}{c+1}\right)$.*

This theorem follows directly from combining the lower bound on the expectation from Eq (7) with the upper bound from Eq (8). And since both the lower and upper bounds leading to this result are obtained first by removing the dependence between trials, we can apply Chernoff bounds to the probability of deviation from this expected value.

3 The Case when Some Bits Guaranteed

Once again, the number of guaranteed bits is $\lfloor\frac{a+b-e}{2}\rfloor$. If we let e_f be the number of cards left in Eve's hand when Alice and Bob are out of cards, then the number of extra bits is $\lfloor\frac{e_f}{2}\rfloor$. Since

initially $a_0+b_0 > e_0$ and at the end of the protocol $a_f+b_f = 0 \leq e_f$, there must be some point at which the two sums cross and $a_i+b_i = e_i$. Specifically this point gives a $(k', k', 2k')$ configuration for some k' (or a $(k'+1, k', 2k'+1)$ configuration, which is asymptotically equivalent). Once that point is reached, we can directly apply Theorem (1) to get that the expected number of extra bits from that point on is

$$\frac{1}{3(1+2)} \cdot k' \leq E\left[B_{f,k} | (k', k', 2k')\right] \leq \frac{2}{(1+2)} \cdot k'$$

Two conclusions fall from this observation. The first is that the crossing point can have e_i at most e_0. Secondly, we can use bounds on the crossing point $(k', k', 2k')$ to give bounds on $E[B_{f,k}]$. Thus $2k' \leq e_0 = kf(k) \rightarrow E[B_{f,k}] \leq \frac{kf(k)}{3}$.

In this section, we use p_m to indicate the probability of a hit (establishment of a bit) and p_e for the probability of a miss (no bit established).

3.1 Configurations where $m \leq e < 2m$

In this section we prove the following theorem:

Theorem 3 *If* $1 \leq f(k) < 2$ *then* $\max(\frac{f(k)-1}{9}, \frac{1}{224}) \cdot k \leq E[B_{f,k}] \leq \frac{kf(k)}{3}$

For any intermediate configuration where $m \leq e < 2m$, we have probabilities $p_m = \frac{m}{e+m} \leq \frac{e}{e+m} = p_e < \frac{2m}{e+m}$. This means that for any series of trials in this range, we expect more misses than hits, and at most twice as many misses as hits. Also note that any sequence of trials with M hits and E misses will decrease m by $M + \frac{E}{2}$ and e by E. This is important because once we establish a gap of $e - m \geq k'$, we expect that any sequence will have at most twice as many misses E as hits M, decreasing m_i to at most $m_i - M - \frac{E}{2} \leq m_i - E$ and e_i to $e_i - E$ which preserves the gap between e and m. Furthermore, Chernoff bounds give that with high probability a gap of size $O(k)$ will not decrease by more than $O(\frac{1}{\sqrt{k}})$. Therefore with high probability once $m \leq e < 2m$, over any long enough sequence of trials, the gap between $m(1+\epsilon)$ and e will not decrease significantly.

The above observation leads to our first lower bound. If $f(k) = 1 + \epsilon$ then $e_0 - m_0 = \epsilon k$. Because of the gap preserving property, with high probability the protocol will cross the $(k', k', 2k')$ threshold with $k' \geq \epsilon k$. Therefore in this case, for any $0 < \epsilon < 1$

$$\frac{k\epsilon}{9} \leq E[B_{f,k}] \leq \frac{k(1+\epsilon)}{3}$$

As $\epsilon \rightarrow 1$ this bound approaches that which we have for $k, k, 2k$ configurations. However as $\epsilon \rightarrow 0$ the lower bound becomes very week. We can improve significantly in the $\epsilon = 0$ case by noting that the first $\frac{k}{4}$ trials create a significant gap (linear in k) with high probability. Specifically, for each of the first $k/2$ trials i from a (k, k, k) configuration $m_i \geq k \cdot \frac{3}{4}$ and $e_i \leq k$. Thus for each of those trials $p_m = \frac{m}{e+m} \geq \frac{3/4}{3/4+1} = \frac{3}{7}$ and conversely $p_e \leq \frac{4}{7}$. With high probability no less than $\frac{k}{4} \cdot \frac{3}{7} - O(\frac{1}{\sqrt{k}})$ of the trials will hit and no more than $\frac{k}{4} \cdot \frac{4}{7} + O(\frac{1}{\sqrt{k}})$ will miss. This produces a gap of at least

$$\begin{aligned}
\left(\text{hits} + \frac{\text{misses}}{2}\right) - \text{misses} &= \text{hits} - \frac{\text{misses}}{2} \\
&\geq \frac{k}{4} \cdot \frac{3}{7} - \frac{1}{2} \cdot \frac{k}{4} \cdot \frac{4}{7} - O(\frac{1}{\sqrt{k}}) \\
&= \frac{k}{28} - O(\frac{1}{\sqrt{k}})
\end{aligned}$$

Thus even with arbitrarily small ϵ, the number of expected bits is still at least a constant fraction of k, more specifically $\frac{k}{28*8} \leq E[B_{f,k}]$ when $1 \leq f(k) \leq 2$. A more careful analysis could improve this constant further. We do not attempt to improve the constant because the important point is that such a constant exists. This completes the proof of Theorem 3.

4 Conclusion

When using the secret key establishment protocol of Fischer et al., the number of secret bits established is often significantly greater than the number of bits guaranteed. This effect is most pronounced when no bits are guaranteed but just barely. In this case, the number of extra bits will be linear in the total number of cards with high probability. The number of extra bits gradually diminishes as the number of guaranteed bits goes up. Since much of the work on this and related problems has focused on the worst case bounds of how many bits are established, the expected number of bits has largely been ignored. As such, one open problem is to devise a deal based secret key protocol that has a higher number of expected bits, though perhaps a weaker (even zero) bound on the number of guaranteed bits.

5 Acknowledgments

I would like to thank Lynn Reggia whose talk on this protocol inspired me to address the problem, William Gasarch who encouraged me along the way, Aravind Srinivasan and Jonathan Katz for their advice on the final writeup, and MohammadReza Ghodsi who checked my calculations.

References

[Che52] Chernoff H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. In *The Annals of Mathematical Statistics* (1952), vol. 23, pp. 493–507.

[FPR91] Fischer M. J., Paterson M. S., Rackoff C.: Secret bit transmission using a random deal of cards. In *Distributed Computing and Cryptography*. American Mathematical Society, 1991, pp. 173–181.

[FW93] Fisher M., Wright R.: An efficient protocol for unconditionally secure secret key exchange. In *Fourth Symposium on Discrete Algorithms: Proceedings of SODA '93* (1993).

[FW96] Fisher M., Wright R.: Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology 9* (1996).

[KMN08] Koizumi K., Mizuki T., Nishizeki T.: A revised transformation protocol for unconditionally secure secret key exchange. *ACM Trans. Comput. Syst.* (2008).

[MW03] Maurer U., Wolf S.: Secret key agreement over a non-authenticated channel. *IEEE Transactions on Information Theory 49*, 4 (Apr. 2003), 822–851.

[Win83] Winkler P.: The advent of cryptology in the game of bridge. *Cryptologia* (1983), 327–332.