Secure computation with a deck of cards

Burton Rosenberg

August 23, 2004
Revised: December 1, 2004

Glossary

x_0	x_1	meaning
♡	♣	0
♣	♡	1
☒	☒	unknown, face down

Five card trick

1. Create the deck, each party keeping their cards face dow.
2. Cut the deck.
3. Turn the cards over and look for pairs of clubs or hearts.

a	b	a_0	a_1		b_1	b_0	$\wedge$	a_0	a_1		b_1	b_0	$\neg\vee$
0	0	♡	♣	♡	♣	♡		♡	♣	♣	♣	♡	♡♡
0	1	♡	♣	♡	♡	♣		♡	♣	♣	♡	♣	
1	0	♣	♡	♡	♣	♡		♣	♡	♣	♣	♡	
1	1	♣	♡	♡	♡	♣	♣♣	♣	♡	♣	♡	♣	

Eight card with committed result

1. Create the deck, each party keeping their cards face dow.
2. Cut the deck.
3. Turn the three top cards over and refer to the table.
   (a) Turn over the two indicated cards or.

(b) Return the three cards face down and cut again.

a	b	$\wedge$	$\vee$	a_0	a_1			b_0	b_1		
0	0	0	0	♡	♣	♡	♣	♡	♣	♣	♡
0	1	0	1	♡	♣	♡	♣	♣	♡	♣	♡
1	0	0	1	♣	♡	♡	♣	♡	♣	♣	♡
1	1	1	1	♣	♡	♡	♣	♣	♡	♣	♡

key			prob	$\wedge$					$\vee$				
♡	♡	♣	1/8	c_0	c_1	⊠	⊠	⊠	⊠	⊠	d_0	d_1	⊠
♡	♣	♣	1/8	⊠	⊠	⊠	c_0	c_1	⊠	d_0	d_1	⊠	⊠
♣	♣	♡	1/8	⊠	⊠	c_0	c_1	⊠	d_0	d_1	⊠	⊠	⊠
♣	♡	♡	1/8	⊠	c_0	c_1	⊠	⊠	⊠	⊠	⊠	d_0	d_1
♣	♡	♣	1/4	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠
♡	♣	♡	1/4	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠	⊠

Oblivious third party test of equality and copying

1. Create a deck $(♡♣)^*$, and cut randomly.
2. Take top two cards from deck and oblivious compare to the unknown pair.
3. If equal, distribute remaining pairs of deck as copies.
4. If not equal, fix by placing top card on bottom and then distribute.

a	b	a_0	a_1	b_0	b_1	$=$
0	0	♡	♣	♡	♣	
1	1	♣	♡	♣	♡	
0	1	♡	♣	♣	♡	♣♣
1	0	♡	♡	♣	♣	♣♣

Analysis as a communication channel

symbol					
A	♡	♣	♡	♣	♡
B	♡	♡	♣	♡	♣
C	♣	♡	♡	♣	♡
D	♡	♣	♡	♡	♣
E	♣	♡	♣	♡	♡

$$\begin{pmatrix} A \\ B \\ C \\ D \\ E \end{pmatrix}_{\text{output}} = \begin{bmatrix} 1/5 & 1/5 & 1/5 \\ 1/5 & 1/5 & 1/5 \\ 1/5 & 1/5 & 1/5 \\ 1/5 & 1/5 & 1/5 \\ 1/5 & 1/5 & 1/5 \end{bmatrix} \begin{pmatrix} A \\ C \\ D \end{pmatrix}_{\text{input}}$$

The input signal $X \in \{A, C, D\}$ is communicated to an output signal $Y \in \{A, B, C, D, E\}$, where we model the cut as loss and noise, $p_{y,x} = P(y \,|\, x) = 1/5$ for all $x \in X$ and $y \in Y$. The full channel includes five other symbols, which we omit. Using Bayes theorem, we find $P(x \,|\, y) =$

$P(x)/(P(A)+P(C)+P(D)) = P(x \mid A \cup C \cup D)$, so from the output we learn nothing beyond our a prior estimates, given that either A, B or C happened.

The eight card trick can be likewise analyzed as a communication channel, to consider what information the channel losses, what noise in injected, and the mutual information between input and output.

References

Valtteri Niemi and Ari Renvall, Secure multiparty computations wihtout computers, Theoretical Computer Science, (191) 1–2, 1998. pp 173–183.

Anton Stiglic, Computations with a deck of cards. Theoretical Computer Science (259) 1–2, 2001. pp. 671–678.