S4 Is All You Need

Donald Beaver

Abstract. A fully shuffled permutation of four cards suffices to implement 1-of-2 Oblivious Transfer at a rate of one transfer per shuffle. After dealing two cards to Alice and one to Bob, Alice deterministically selects item from a three-fold partition of the edges of a tetrahedron, at which point OT is established. Unlike decades of 2-player computation results employing restricted permutations (as in den Boer's groundbreaking Five Card Trick) and artificial decks with repeated symbols, the "Tetrahedral OT" is the first to achieve two-party secret computations using a *fully-shuffled set of unique elements*. New "tenancy" and "narrowing" techniques are developed. Design patterns and protocol generation parameters are presented, along with some insightful but less efficient choices. The geometric symmetries behind the Tetrahedral OT protocol open up connections from Oblivious Transfer to Secret Key Exchange protocols as well. Decoupling information-theoretic permutations from computational one-wayness provides systematic access to broader and novel MPC protocol design, insight and simplification.

Keywords: oblivious transfer · multiparty computation · combinatorial protocols · card-based cryptography · graph theory · tetrahedron · information-theoretic security

1 Introduction

Card-based cryptography provides elegant insights into the natural symmetries of cryptographic protocols, isolating the "hiding" or one-wayness aspects from the "permuting" aspects. While holistic one-way trapdoor permutations suffice for broad swaths of cryptographic applications, entirely new architectures arise when one is free to apply hiding and permutational aspects at different stages and using different resources. Correlated pseudorandomness, PCGs, Oblivious Transfer generation, BMR-style multiparty protocols – these are all architectures where one-wayness achieves one goal and information-theoretic permutations (implemented as correlated seeds or as algebraic secret shares) achieves another.

Landmark results from the 1980s and 1990s established surprising and extractable sources of correlated randomness from shuffled decks of cards, suitable for secret key exchange (SKE) and for two-party computation (2PC).

Tenancy Games on Standard Decks for SKE. The Fischer-Patterson-Rackoff-Winkler-Wright line of research showed how fully-shuffled standard decks of unique cards establish key exchange between parties each holding a hand of cards [15, 16, 38]. The simplest intuition behind these protocols is for Alice to announce something along the lines of "Hey Bob, our secret bit b is 0 if I'm holding the Ace of Spades." When Bob holds the Ace of Spades, he easily infers $b = 1$.

And of course, when Bob lacks $A\spadesuit$, he infers that Alice has it – but wait, we need a little more in a protocol for this to work. The brilliance behind FPRW protocols is to first narrow the public knowledge down, via open conversation, to a pair $\{A\spadesuit, A\heartsuit\}$ of cards where Alice holds one, Bob holds the other, but the eavesdropping public doesn't know which.

The final, secret outputs of the protocol depend on asymmetric knowledge of the *tenancy* of the cards. Alice and Bob know the tenancy, but Eve doesn't.

A related line of SKE research based on Winkler's foundational work in securing the game of Bridge dove deeply into the combinatorics behind establishing a shared secret from any structure representing shared knowledge between Alice and Bob [5, 36, 38]. The now-standard cryptographic game involves two sheriffs from neighboring towns, each holding a list of suspects and having identified one, wishing to narrow their list privately to a pair of guilty individuals. There are local lynch mobs but they have integrity: they won't lynch a suspect if there is any possibility of innocence. The Two Sheriff's must communicate carefully over wiretapped lines. Research in this line established graph-theoretic properties characterizing overlapping-knowledge scenarios when the sheriffs can succeed. Narrowing joint information is again a theme but in a somewhat different way: the sheriffs narrow to multiple sets of possibilities.

The Tetrahedral OT protocol in our current work builds on the FPRW line of research, extending it with novel encodings needed to achieve coordinated oblivion, and introducing a wholly new, randomized set-narrowing reminiscent of Two Sheriff's games, but applied in non-obvious ways and for the first time to 2PC/OT.

Bespoke Decks and Shuffles for 2PC/OT. Den Boer established a surprising second line of protocols in which 2PC-Alice and 2PC-Bob[1] can play Tinder, i.e. establish $c = a \wedge b$ secretly, using five cards ($\{\heartsuit, \heartsuit, \heartsuit, \spadesuit, \spadesuit\}$) [7]. Alice and Bob start with $\{\heartsuit, \spadesuit\}$ in their hand. The essence of the protocol is to put a face-down $\heartsuit$ in the middle and for each party to vote (1) *Yes* by playing a face-down $\heartsuit$ next to it (resp. (0) *No*, by playing $\spadesuit$), then putting the remaining card further away. The protocol relies on circularly rotating the five cards (implemented as cutting the deck), after which the output is 1 iff there are three hearts in a row.

What is distinctive about den Boer and the ensuing line of research into 2-player AND/OT/f(x,y) protocols is that they use uniformly random permutations from a *subset* of all possible permutations, and they use repeated card symbols. A cut of a deck is a random rotation, namely a random choice from a subgroup of permutations, C_n, but it is not an arbitrary permutation.

A long line of ensuing research has explored the power of subgroup permutations with repeated symbols [7, 19, 23, 25, 27, 29, 31]. In contrast to tenancy-style protocols, the partly-randomized state of a common object (e.g. a deck built with contributions made by players) represents the outcomes, rather than what cards are held by which parties.

In fact, there has seemed to be intuitive evidence that full shuffles of unique cards are perhaps too chaotic and too singular to be employed in computation-seeking protocols.

[1] To skirt confusion among the "Alices" and "Bobs" of SKE and 2PC, we'll often mention them as "SK-Alice," "SK-Bob," "2PC-Alice" "2PC-Bob,", "OT-Alice," "OT-Bob."

Crépeau and Kilian introduced Solitary Games, in which Alice uses face-down cards and cyclic shuffles (cuts) to simulate a discreet counterparty [12]. They conjectured that everyday full-permutation shuffles would scramble too intensively to support Solitary games. An absence of full-shuffle approaches to 2PC protocols in the literature likewise suggests a similar, implicit impotence.

Tenancy Games on Standard Decks for 2PC/OT. This paper demonstrates, in contrast, that *full-shuffle unique-card protocols* can power 2PC as well as (long-established) SKE. What's more, our "tetrahedral" OT illustrates a deep connection between the secret message bit in SKE and the secret selection bit in $\binom{2}{1}\mathtt{OT}$. Establishing a secret s between Alice and Bob in SKE corresponds to establishing the secret selection s known only to Bob and Rob in OT.

What's that? Who's Rob? OT-Rob is a poetically-licensed entity who stole the bit that OT-Bob didn't get (in OT). We'll expand on this trope later, but the leftover deck after hands are dealt is essentially a silent, imaginary, extra player, a bit like a Bridge dummy. OT-Alice sends m_s to OT-Bob and $m_{s'}$ to OT-Rob (the deck). This perspective is interesting not just as a way to harvest OT architectures from SKE architectures (and back) but is also profitable when considering quantum settings, where substates are permuted and dealt in unclonable and non-erasable paths along different wires to different custodians.

The tetrahedral group ties it all together, establishing a rate-1 stream of $\binom{2}{1}\mathtt{OT}$ from a $log_2 4! = log_2 24 = 4.58$ bit injection of randomness, of which $log_2 3 = 1.58$ bits are discarded by announcing them publicly in a single-message narrowing step, leaving 3 hidden bits (c, m_0, m_1) to support $\binom{2}{1}\mathtt{OT}$.

The tetrahedron itself provides a simple visualization for the protocol and for the "wires" along which m_s and $m_{s'}$ travel. The symmetries are beautiful, illustrative and informative, like secret sharing, like RSA, like a one-time pad. We show:

Theorem 1. *(Tetrahedral OT) Dealing 2 cards to Alice and 1 card to Bob from a fully-shuffled deck of four unique cards suffices to implement* $\binom{2}{1}\mathtt{OT}$ *with a deterministic protocol, secure against semi-honest adversaries.*

The protocol is simple to execute and the theorem is simple to prove. It almost appears to be a staggeringly inexplicable and lucky coincidence, when viewed merely by its rules and proof, though. This work makes several other contributions by expanding the strategies of early tenancy games, showing also how coordinated tenancy games help reach beyond the "simple" world of SKE, making connections to design patterns found in uncertainty games, and describing parametric choices explaining the protocol rules (and a family of variants, and the symmetries among them) in the first place.

Roadmap. Section 3 presents Tetrahedral OT. Section 4 analyzes it. Section 6 connects it to geometry. Section 7 connects it to graph theoretic approaches to combinatorial secrecy. Section 8 describes a simpler but weaker variant. Section 9 applies Tetrahedral OT to larger decks. Section 10 concludes.

2 Notation

Definition 2. *A* deck $\mathcal{D}$ *is a multiset over an alphabet* $\mathcal{A}$*. A* simple deck $\mathcal{D}(n)$ *is just* $\{0, 1, \ldots, n-1\}$*. The* French Deck *is* $\mathcal{D}(52)$*.*

Definition 3. *A* deal $(h_1, \ldots, h_H; d)$ *is a partition of a deck of size* d *into a specified configuration of* $H+1$ *multisets, called hands, having respective sizes* $h_1, \ldots, h_H, h_{H+1}$*. The last hand* $(H+1)$ *is called the discard pile, remaining deck, or discard deck. An* ordinary deal *is the probability distribution (or sample thereof) obtained from a uniform shuffle of deck* $\mathcal{D}$ *followed by partitioning into the hands of the specified size.*

Thus, a $(n_a, n_b; n_d)$ deal uses a random permutation from S_n, $n = n_a + n_b + n_d$, with the first n_a elements communicated to Alice, the next n_b to Bob, and the last n_d left in the discard deck pile (aka silent Rob). In this work, we focus on $H = 2$ players, Alice and Bob, with a $(2, 1; 1)$ deals or a French deck $(13, 13; 26)$ deal.

In this work, there is nothing particularly special about a French deck (52 cards, 4 suits, 13 ranks), although it coincidentally happens to have 4 unique suits, making it of pragmatic interest for compositions of the Tetrahedral protocol.

S_n, the symmetric group on n elements, C_n the cyclic group. C_n is implemented in card games as a mathematically random cut. (A real-world cut usually omits the identity, but card protocols all include it.)

Definition 4. $\binom{2}{1}\mathsf{OT}$ *is the chosen 1-of-2 Oblivious Transfer primitive, in which Alice provides two bits* m_0, m_1 *and Bob provides a selection bit* s*, and Bob learns* m_s *(but nothing about* $m_{s'}$*) while Alice learns nothing.*

Definition 5. $\frac{1}{2}\mathsf{OT}$ *is the 1-of-2 Oblivious Transfer primitive, in which Alice provides two input bits* m_0, m_1 *and Bob receives a random selection bit* s*, and Bob learns* m_s *(but nothing about* $m_{s'}$*) while Alice learns nothing.*

Definition 6. $\frac{1}{2}\mathsf{ROT}$ *and* $\binom{2}{1}\mathsf{ROT}$ *are the random selection variants of* $\binom{2}{1}\mathsf{OT}$ *and* $\frac{1}{2}\mathsf{OT}$*, respectively, in which Alice receives two random bits* m_0, m_1 *and Bob learns a random selection bit* s*, and Bob learns* m_s *(but nothing about* $m_{s'}$*) while Alice learns nothing.*

A series of results shows that these variants are easily interchangeable, reversible and precomputable, so we will often refer to 12OT to mean any of them. [3, 13, 14, 39]

For presentation and even real-world implementations, it can be convenient to portray $\{0, 1, 2, 3\}$ as $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. Again, there is nothing magical or mathematically significant here, just a pleasant convenience.

If the reader has a color presentation, the "channel 0" values are colored red while the "channel 1" values are black. (If not, channel 0 is presented on the left, channel 1 on the right.) One may be tempted to interpret this as red-black suits, but (apart from a weaker protocol discussed later) this is not generally the case and in fact can detrimental to pursue. The "magical coincidence" of four suits, two of which are red and two black, can misdirect us into poorer constructions, which is why magical coincidences should be taken with a grain of sleight.

3 Tetrahedral OT Protocol

The simplest description of the Tetrahedral Protocol is as a 2PC protocol for $\binom{2}{1}\texttt{ROT}$ on a $(2,1;1)$ deal, shown in Fig.3. Other variants of OT are straightforward modifications. [3, 13, 14, 39]

Start with a deck of 4 unique cards, 0, 1, 2, 3, shuffled uniformly with a random permutation $\rho \leftarrow S_4$. Alice will learn random input bits (m_0, m_1), and Bob will learn a random selection bit s along with m_s.

Alice's message M is a log 3-bit string (sure, she does need a 2 bit message to send it) from $\{X, Y, Z\}$, and Bob's output is a pair of bits (y_0, y_1).

Alice and Bob are purely deterministic. The deck is the only source of randomness. Alice and Bob consult the tables in Fig.1 and Fig.2 to determine what to say and to conclude.

A	0	1	2	3
0	·	Z 11	X 11	Y 10
1	Y 11	·	Y 01	X 00
2	Z 10	X 01	·	Z 00
3	X 10	Z 01	Y 00	·

Fig. 1. Tetrahedral Alice for hand $(\rho(0), \rho(1))$, giving message M and bits m_0, m_1.

B	0	1	2	3
X	0•	1•	•0	•1
Y	0•	•0	1•	•1
Z	0•	•0	•1	1•

Fig. 2. Tetrahedral Bob for incoming message $M \in \{X, Y, Z\}$ with hand $\rho(2)$, giving outputs y_0, y_1.

1. Randomly sample $\rho \leftarrow S_4$.
2. Deal $(\rho(0), \rho(1))$ to Alice, $\rho(2)$ to Bob.
3. Alice consults Table A on $(\rho(0), \rho(1))$ to utter $M \in \{X, Y, Z\}$ and record m_0, m_1.
4. Bob consults Table B on $(M, \rho(2))$ and records (y_0, y_1).

Fig. 3. The Tetrahedral Protocol for $\frac{1}{2}\texttt{ROT}$ on a $(2,1;1)$ deal.

4 Security Proof

We show that Tetrahedral protocol of Fig.3 implements $\binom{2}{1}\texttt{ROT}$ on a $(2,1;1)$ deal, from which Theorem 1 follows immediately. A more intuitive exposition illustrating the symmetries, geometries and intuitive reasoning behind the protocol appears in later sections, but here we let the numbers prove the pudding. The transcripts, joint and marginal distributions, and output cases have all been vetted by hand and automation.

Theorem 7. *(Tetrahedral ROT) The protocol of Fig.3 implements* $\binom{2}{1}\texttt{ROT}$ *securely against semi-honest adversaries.*

Proof. Since Alice and Bob are deterministic, there are 24 equally likely protocol transcripts, one for each permutation of the deck. The tables are constructed to ensure that $y_s = m_s$ for all 24 permutations, making correctness of the outputs trivial to check. (Specifically: there are no contradictions between m_0m_1 and y_0y_1.)

ρ	M	m_0m_1	y_0y_1
0123	Z	11	•1
0132	Z	11	1•
0213	X	11	1•
0231	X	11	•1
0312	Y	10	•0
0321	Y	10	1•

ρ	M	m_0m_1	y_0y_1
1023	Y	11	1•
1032	Y	11	•1
1203	Y	01	0•
1230	Y	01	•1
1302	X	00	0•
1320	X	00	•0

ρ	M	m_0m_1	y_0y_1
2013	Z	10	•0
2031	Z	10	1•
2103	X	01	0•
2130	X	01	•1
2301	Z	00	0•
2310	Z	00	•0

ρ	M	m_0m_1	y_0y_1
3012	X	10	1•
3021	X	10	•0
3102	Z	01	0•
3120	Z	01	•1
3201	Y	00	0•
3210	Y	00	•0

Fig. 4. Tetrahedral transcripts. $s = 0$ is denoted by a right dot, $s = 1$ by a left dot.

First, consider Alice's view. For any pair m_0m_1, there are precisely 6 transcripts producing it. Thus her outputs are uniformly random. Moreover, of these 6 transcripts, there is a pair of cases for each $M \in \{X, Y, Z\}$. For each of those pairs, one produces $s = 0$ and the other produces $s = 1$, so s is independent of Alice's view. The diligent reader can inspect (0123, 0132), (0213, 0231), (1023, 1032), for example.

Next, consider Bob's view, produced by a particular M and $\rho(2)$. There are 12 cases, and in each case, there is a pair of transcripts producing it. Let $s' = 1 - s$. For each such pair, one produces $m_{s'} = 0$ and the other produces $m_{s'} = 1$, so $m_{s'}$ is independent of Bob's view.

$M, \rho(2)$	ρ	m_0m_1	ρ	m_0m_1	y_0y_1
$X0$	1302	00	2103	01	0•
$X1$	0213	11	3012	10	1•
$X2$	1320	00	3021	10	•0
$X3$	0231	11	2130	01	•1
$Y0$	1203	01	3201	00	0•
$Y1$	0312	10	3210	00	•0
$Y2$	0321	10	1023	11	1•
$Y3$	1032	11	1230	01	•1
$Z0$	2301	00	3102	01	0•
$Z1$	2013	10	2310	00	•0
$Z2$	0123	11	3120	01	•1
$Z3$	0132	11	2031	10	1•

Fig. 5. Bob's marginal distribution, with two consistent shuffles per row.

This is slightly trickier to verify by hand, so we tabulate the marginal distribution explicitly in Fig.5. For any $M \in \{X, Y, Z\}$ and hand $\rho(2)$, there are precisely 2 transcripts.

By inspection, there is one value of s for which both transcripts produce the same m_s, and an opposite value s' for which the transcripts produce different $m_{s'}$. As each entry of the table is uniformly random, $m_{s'}$ is independent of Bob's view.

For the diligent reader, consider $Y3$ (Alice said Y and Bob drew 3), for example. The results for 1032 and 1230 are $m_0 m_1 = 11$ and 01, thus $s = 1$ and $m_{s'}$ is independent of Bob's view. □

5 Expanded and Coordinated Tenancy Games

The Tetrahedral OT protocol pioneers the first and a necessarily expanded application of tenancy games, in which secret values are determined by establishing which players hold certain cards. Tenancy games, introduced by Fischer, Patterson, Rackoff, Winkler and Wright to address SKE, follow two general steps:

- *Narrowing:* The parties exchange public messages to narrow common knowledge to a useful state.
- *Tenancy:* The parties use the narrowed state to establish a secret value by virtue of who holds which card.

The Tetrahedral OT protocol extends this pattern in two ways:

- *Predicate Tenancy:* the narrowed state depends on a predicate of the card values themselves.
- *Coordinated Tenancy:* two or more tenancy games run simultaneously.

To whet the intuition: the *predicate tenancy* uses statements of the form, "1 if Alice holds the larger of the cards in a private set S known just to Bob." The term *larger* is a stand-in for a suitable predicate depending on card values, not merely who holds a particular, fixed card. ("Larger" itself can be a design dead-end.) The essential distinction is that prior tenancy games arranged to announced the narrowed set S publicly. Today, we keep it somewhat secret, which does seem to inhibit the classical mic-drop final step in SKE, but it helps in OT.

With *coordinated tenancy*, we can run two or three tenancy games at once. In particular, Alice and Bob run one game using set S (as mentioned, no longer universally public.) Alice and Rob run another game using a different set S'. Recall that Rob is the silent deck, an imagined particpant, the OT transmission channel leading away from Bob. When Alice's utterances function as messages to *Rob*, they represent a coordinated tenancy game where Rob, if reified and holding the undealt deck itself, would be capable of learning the obliterated message $m_{s'}$.

These intuitions are likely to become more clear with the geometric, tetrahedral representation of the protocol. A key insight, for now, is that Tetrahedral OT establishes three simultaneous tenancy games:

- one game for m_0 (secret between Alice and Bob, hidden from Rob),
- one game for m_1 (secret between Alice and Rob, hidden from Bob),
- one game for s (secret between Bob and Rob, hidden from Alice).

5.1 Concrete Example: Simple Tenancy

Let's take a spin with SKE approaches and see whether they extend to OT. In the traditional SKE setting, a 3-card deal suffices: a_0 to SKE-Alice, a_1 to SKE-Bob, and a_2 to an eavesdropper. Alice picks and announcese a 2-set S containing a_0, namely either $\{a_0, a_1\}$ or $\{a_0, a_2\}$. If lucky, $a_1 \in S$. Bob says whether his card is in S, and if not, they restart with a new hand.

When a suitable S has survived rejection sampling, Alice picks $x \leftarrow S$ randomly and says, "The secret bit m is 1 if Alice holds x." Eve, even holding the third card, cannot tell whether Alice or Bob holds x, so the secret remains unknown to her. This is the brilliant move in tenancy protocols.

Now, let's try this style with OT-Alice and OT-Bob. We quickly realize that OT-Alice and OT-Bob aren't really trying to establish a secret. In particular, if OT-Alice successfully "transmits" to OT-Bob using some pair S, she knows whether OT-Bob got the message.

Maybe OT-Bob can remain silent, so that Alice doesn't discover whether S would have been rejected, and Bob learns m precisely in those cases S is acceptable. With a 50 percent chance of either case, we seem to have obtained Rabin OT on a random message input. This is progress, as Rabin OT is sufficient for 2PC, although it is expensive when used to build $\frac{1}{2}\mathtt{OT}$.

5.2 Coordinated Tenancy via Potentially Mixed SKE

Given a 4-card deck and a $(2, 1; 1)$ deal of a_0, a_1 to SKE-Alice and a_2 to SKE-Bob, the results of FPRW might have Alice announce a 2-set S containing one card she holds and one card she doesn't. Specifically, she might choose $\{a_0, a_2\}$, $\{a_0, a_3\}$, $\{a_1, a_2\}$, or $\{a_1, a_3\}$. Alice announces S. If $a_2 \in S$, Bob confirms success. Alice picks $x \leftarrow S$ randomly and says, "The secret bit m is 1 if Alice holds x." Eve, even holding the fourth card, cannot tell whether Alice or Bob holds x, so the secret remains unknown to her.

In particular, Bob ought not confirm whether S is rejectable. In fact, by coordinating two tenancy protocols in parallel, using S and S' (a partition of the four cards), Bob may see S as a failure while S' is meaningful, in terms of successfully transmitting a bit.

With this choice of decks and pattern of coordination, we can build $\frac{1}{2}\mathtt{ROT}$, as long as Alice or Bob have suitable private streams of random bits to invest.

5.3 Derandomized Coordination

The Tetrahedral protocol is "deterministic" in that neither OT-Alice nor OT-Bob need to bring random bits to the protocol. There is randomness, however, supplied by the shuffle.

If protocol designers seek to minimize resource usage, however, there are pitfalls to consider. If Alice is instructed to choose a given S based on her hand, an attacker really only cares under what circumstances Alice announces "Let's use S and S'." The overall protocol must be analyzed to see whether any other circumstances give rise to a particular S. Naturally, this is necessary for a security proof, but from the design

standpoint, it doesn't help much in the process of defining a candidate and maximally-derandomized set of instructions for Alice.

The Tetrahedron OT protocol needs no external randomness. It is not clear from a naive application of SKE tenancy ideas that such maximal derandomization will be possible, let alone how to achieve it. We now turn to the geometric patterns giving Tetrahedral OT its name, to see how there is sufficient natural randomness in the shuffle alone.

6 The Tetrahedron

While the tables in Fig. 1 and Fig. 2 suffice to define and prove the Tetrahedral OT protocol, they shed little human or general mathematical understanding. Here, we visit geometric symmetries and tie them to coordinated tenancy protocols. This foray is not the proof of the protocol (although in many settings it might be accepted as such); it is informational, to understand design and intent and provide intuition for further protocol design.

Fig. 6 portrays a tetrahedron with four standard vertices, $\{v_0, v_1, v_2, v_3\}$ at natural coordinates: $v_0 = (1, 1, 1)$, $v_1 = (1, -1, -1)$, $v_2 = (-1, -1, 1)$, $v_3 = (-1, 1, -1)$. Each vertex corresponds to a card from $\{0, 1, 2, 3\}$ (or $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$).

The six edges of the tetrahedron can be partitioned into three pairs of opposing, skew edges. Each edge pair is perpendicular to one of the three coordinate axes, so we label them X, Y, and Z: We denote them as $X = \{v_0, v_1), (v_2, v_3)\}$, $Y = \{v_0, v_2), (v_1, v_3)\}$, $Z = \{v_0, v_3), (v_1, v_2)\}$.

For example, the X-edge (v_0, v_1) is perpendicular to the x-axis, at $x = 1$ to the right, and its partner X-edge (v_2, v_3) is skew to it, perpendicular to the x-axis, at $x = -1$ to the left. These edges are colored red in Fig. 6. All three pairings are shown in Fig. 6.

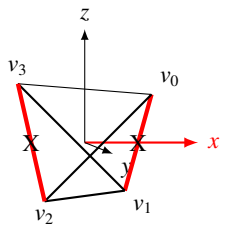


Fig. 6. Illustrating the "X" pair, (v_0, v_1) and (v_2, v_3), of opposing, skew, tetrahedral edges.

6.1 Geometry of the Protocol

Let's now look at how and whether we might use tenancy patterns (rejecting eavesdroppers by keeping them ignorant of who holds which cards in a set) to build OT using these tetrahedral concepts.

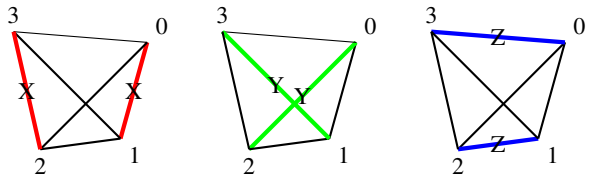


Fig. 7. The three pairs of skew edges, colored red, blue, and green.

These skew sets are essentially communication channels in the Tetrahedral OT protocol. Based on her dealt hand, OT-Alice picks one of the three sets to use for transmission, intending to establish tenancy-style transmissions for two bits m_0, m_1.

Bob holds a distal card on exactly one edge, so if tenancy-style transmission holds, he can learn one of the bits. Lacking knowledge of who holds which cards on the other edge, he fails to discover the other bit.

Now, Alice should not learn which of these two is the case. This makes life a *little tricky* for her compared to SKE tenancy protocols, where the counterparties know everything about the transmission they are trying to establish. She cannot naively use SKE approaches because she doesn't know who her counterparty is. If a draft protocol employs SKE-style feedback from Bob, like rejection sampling, then Alice might learn of Bob's particular interest in one message or the other.

Continuing: there is a pleasant symmetry when we regard Bob as holding one card and Rob holding the other. Bob becomes, essentially, an eavesdropper on the edge he's not adjacent to, where Rob would ultimately discover the other message, remaining ignorant of Bob's. In *hindsight*, we might even conclude a Silent Bob is *necessary*, because the natural counterparty Rob cannot speak. (This is an observation, not a proof.)

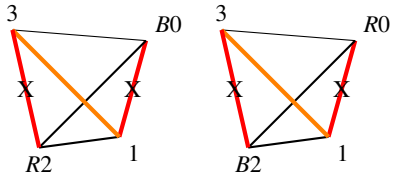


Fig. 8. Example trial for Alice, sending "X" on a $(1, 3)$ deal. Bob might have 0 or 2.

Now, concretely, let's say OT-Alice was dealt $(1, 3)$. She might pick the X-channel by announcing "$M = X$." Translating, she is essentially saying: "I hold one card on each of the red X-edges." In Fig. 8, Alice's orange edge $(1, 3)$ is coupled to each of the red X-edges.

Aside: Caution, a Contextual Interpretation Pitfall. It's a deep, subtle pitfall to design protocols using quoted messages which a human interprets as being true on their face. Alice's actual message is "X" – not a four-dozen character ASCII string which itself,

merely by declaring something in English, makes its English interpretation true. It is only by inspecting the circumstances under which "X" might be uttered that we can ascribe semantic implications [5]. Concretely, if this were the only circumstance under which Alice says "X," then she really would be conveying, "I hold $(1, 3)$," even if the protocol author dictated that she say "I hold one card on each of the red X-edges." But let's continue intuitively for now, confident that we have already fully specified and proved the final Tetrahedral OT protocol anyway.

The Z-channel also looks viable for Alice to use, impinging on her hand $(1, 3)$ in separate ways such that Bob holds exactly one of the two Z-edges. The Y-channel, however, becomes fruitless for a tenancy-style protocol: there are no vertex-sets in which both Alice and Bob hold a card.

Thus, a general and intuitive pattern emerges: if Alice's hand is in Y, she can potentially use X or Z to proceed. Likewise, for any of the three: if Alice's hand is in $W \in \{X, Y, Z\}$, then she should consider $\{X, Y, Z\} \setminus W$.

6.2 Picking Channels

We might be tempted to employ a rock-paper-scissors pattern to choose the skew set. Say, if Alice holds W then she announces $W + 1 \mod 3$. Namely, if she holds a hand in X, say "Y"; if she holds a hand in Y, say "Z"; etc.

On deeper inspection, say she does hold a hand in Y and always says "Z." Then Bob, holding 2, can observe that Alice does *not* hold $\{0, 2\}$, so he *concludes* she holds $\{1, 3\}$. He would learn one message from the $(1, 2)$ channel, but knowing that Alice holds the 3 in the $(0, 3)$ channel, he learns the other message too. Basically, he knows everything about the deal: what cards Alice holds, what he holds, and what remained undealt.

(*Often Overlooked Subleties:* When Alice holds *rock*, she says "not rock"? Well, she can't do that! The only time she'd say, literally, "not rock" is when she *does hold rock*, a contradiction and not much help. This is the Contextual Interpretation Pitfall again.)

We are almost ready to conclude that Alice needs to say "Z" some of the time and "X" some of the time, if this direction is to succeed. Maybe Alice can just choose at random. How would this help?

If Alice chooses something from "not-W" uniformly at random, we can make things work. On hearing "Z," Bob concludes in turn only that it is equally likely that Alice's hand came from X or Y. His Bayesian inference is blocked.

This symmetry is baked into the Tetrahedral OT protocol and is a key part of its design.

6.3 Tenancy and Novel Predicate Encoding

We're not there yet. As mentioned, the SKE protocols often have Alice mentioning a specific card in a public set S, like "If I hold $A\spadesuit$..." Because SKE-Bob is intended to learn results, SKE-Alice can certainly say things he might learn anyway. When we try to apply such patterns to OT, there are dangers. Alice might naively state things that would not violate the SKE-style security of m_s given to Bob but which might lead to inferences about $m_{s'}$. There are cases similar to the "not rock" problem above, where

Alice's mention of a coordinating set S (e.g. directly mentioning $A\spadesuit$) would lead to understanding exactly which *other card* she holds on the edge not privy to Bob. Because those situations are not addressed by SKE (a single SKE doesn't care about other protocols in play), more care is needed.

To this end, we wish Bob to understand what is encoded on channel s for the edge he holds one card, but the encodings must not leak what is encoded on the other channel s'. Specifically, the encodings must be chosen so that on channel s', Bob fails to learn $m_{s'}$. The only plausible way to achieve this is to arrange $m_{s'}$ to "vary" according to Bob's ignorance of Rob's tenancy: namely, ignorance of what card remained undealt and what card Alice holds.

If Alice has $(1, 3)$, said "X," and Bob has 2, then from Bob's view, he knows Alice has 3 but thinks Alice might also hold 1 or 0. Notably, for Bob, Alice would also have said "X" if she had $(0, 3)$. By construction, Bob remains ignorant. The output bit for the s' case should vary accordingly. See Fig 6.3.

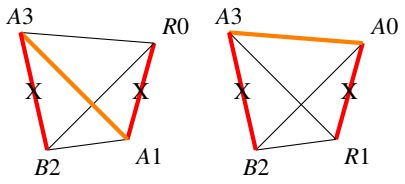


Fig. 9. Two deals consistent with Bob holding 2: Alice said "X," holding $(1, 3)$ or $(0, 3)$.

Thus, we need a tenancy encoding which varies suitably under certain circumstances, which does not inadvertently reveal itself via a "not rock" scenario, and which establishes a bit m_s for OT-Alice and OT-Bob to agree upon, while also establishing a bit $m_{s'}$ for OT-Alice and OT-Rob to agree upon.

We thread this needle by stepping away from mentioning concrete values in the tenancy sets. Instead, we use broader interpretations such as "the secret is 1 if Alice holds the *larger*" or more precisely, "The secret is 1 if $R(x_a, x_b)$ holds" for a *antisymmetric* predicate R applied to Alice's and Bob's cards.

Specifically, Alice holds x_a, Bob holds x_b, but neither x_a nor x_b is ever mentioned - *unlike earlier SKE card protocols*.

The application of this antisymmetric predicate is baked into the Tetrahedral OT Protocol and can certainly be reverse-engineered from Alice's conclusions m_0, m_1.

6.4 Combining and Derandomizing

Putting these concepts together, the flow is as Fig. 10 describes. Alice sends a random skew-pair, Bob learns that Alice holds x_a for one edge, and deciphers m_s.

To derandomize, note that Alice can use her ordered hand $(\rho(0), \rho(1))$ to provide the skew-choice bit. Just settle on another antisymmetric predicate, $Q(i, j)$ and choose accordingly. For example, $Q(1, 3) \neq Q(3, 1)$, so the random shuffle of $\{1, 3\}$ gives a bit

actionable by Alice but unknown to Bob. Bob doesn't know if Alice got 1 before 3 or 3 before 1, enough to keep him ignorant of the origin of Alice's message.

1. Randomly sample $\rho \leftarrow S_4$.
2. Deal $(\rho(0), \rho(1))$ to Alice, $\rho(2)$ to Bob.
3. Alice finds the $W \in \{X, Y, Z\}$ which contains $(\rho(0), \rho(1))$, then sends a random message $M \in_R \{X, Y, Z\} \setminus W$.
4. On $W = \{P_0, P_1\}$, Bob calculates s for which $\rho(2) \in P_s$.
5. Bob deduces x_a from $P_s \setminus \rho(2)$.
6. Bob uses $R(x_a, \rho(2))$ to decode m_s.

Fig. 10. Geometric-combinatoric informal description of Tetrahedral OT

7 Combinatorial Graph Theory Connections

While the vast majority of SKE and OT protocols are analyzed in terms of probabilities and information theory, a branch of protocol analysis considers a more moderate stance: whether an attacker merely faces an uncertainty of sorts. The uncertainly-focused line of analysis does not try to quantify relative likelihoods or uncertainties. It merely settles issues of whether someone can act with certainty on particular claims.

Uncertainty is important for at least two reasons. First, the cost of a failure may be unacceptable, as in the case of executing an innocent person, or causing an entire financial system to fail. Second, even apart from moral or pragmatic costs of failures, knowing what cannot be achieved with certainty allows us to rule out perfectly information-theoretically protocols.

That is, if the steps of a draft protocol can be shown to fail to leave *desirable uncertainties*, then we can rule out further work on the draft. For example, a draft protocol which fails to leave an eavesdropper with uncertainty over an established key can be disregarded (again: when one is seeking perfectly secure protocols).

Winkler *et al* considered graph structures representing overlapping facts shared partly by Alice and partly by Bob, with regard to establishing shared knowledge that leaves Eve uncertain. The typical example is the Two Sheriff's Problem. Alice has a list of suspects, nodes on a bipartite graph, as does Bob. Each one knows a guilty suspect, and thus there is an edge on the bipartite graph connecting the two suspects and representing the actual full facts of the world. There are other edges connecting other plausible pairs of suspects as well. [5, 38]

As long as Alice and Bob can narrow Eve's beliefs to the *possibility* that two disjoint edges (a_0, b_0) and (a_1, b_1) might either be true, then they are able to understand which of those edges represents reality. In cryptographic application, they have one "bit" (not information-theoretic) known to them (i such that (a_i, b_i) is factual: a kind of tenancy protocol) but uncertain to Eve. Note that a protocol has to leave Eve uncertain no matter which edge in a graph is called factual; this is a strongly combinatorial setting.

Eve's decent lynch mob, or ordinary justice system, or life-stakes bet, will be prevented from acting by the tiniest uncertainty. Again: this is not meant to be "quantifiable."

When a mutual-knowledge graph supports a protocol, one can undertake further investigation to see if information theoretic probabilities can be balanced properly.

When the graph structure cannot support a protocol, we know *there will not be* an information-theoretic solution either.

In the current work, we apply this Winkler-style uncertainty analysis to graphs representing mutual knowledge in OT but in a far more challenging manner than SKE. Here, we need to preserve uncertainties in three areas simultaneously: Alice's *uncertainty* over s, Bob's *uncertainty* over $m_{s'}$, and Rob's *uncertainty* over m_s.

7.1 The Star of OT

Consider a bipartite graph, which we will draw with Alice's vertices on an outer circle and Bob's on an inner circle. Each vertex represents a possible item of knowledge for Alice or for Bob. Every edge represents a possible combined situation in the world.

1-of-2 Oblivious transfer is represented as a four-pointed star. Alice has four possible message pairs, and Bob has four possible results (two for s, two for m_s). See Fig. 11. A dot on the left means $s = 1$, while a dot on the right means $s = 0$.

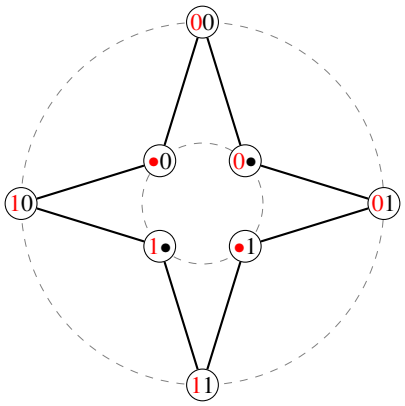


Fig. 11. Bipartite knowledge graph for 12OT.

Formally, each of these edges must be equiprobable to satisfy the requirements of 12OT. In the "uncertainty" domain, each of these edges must at least be a possibility.

Any protocol which narrows (and eventually uses tenancy to declare the results) a starting configuration to an OT-star graph must at the very least leave uncertainties, else it cannot hope to leave nonzero and balanced probabilities.

This informs our design efforts.

7.2 The Star of S4

The knowledge graph for a $(2, 1; 1)$ deal of 4 cards shuffled uniformly by an S_4 permutation is slightly more intricate but no less attractive. Alice has 12 possible vertices, corresponding to each of $4 \cdot 3$ pairs she can be dealt. Bob has 4 possible vertices, corresponding to each of 4 singlets he can be dealt. Star, tetra star, flower, sunflower, wretched mess: the graph is shown in Fig. 12.

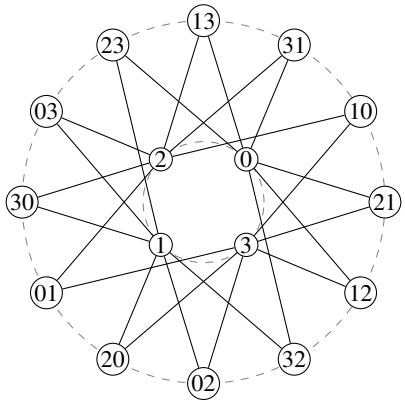


Fig. 12. Bipartite knowledge graph for S4 deal of 2 to Alice, 1 to Bob.

7.3 Narrowing to OT Subgraphs

The "narrowing" conversation we seek is for Alice and Bob to send messages which reduce the tetra star's 12x4 mess down to a simple 4x4 OT star.

We need to drop down by a factor of 3. The messages $\{X, Y, Z\}$ of the Tetrahedral OT protocol correspond to choices among three distinct 4x4 subgraphs of the tetra star.

For example, we can choose a blue subgraph as drawn in Fig. 13 and have Alice say "Z" when she holds any of the four combinations on the outer ring. In the figure, note that Alice's $m_0 m_1$ are now marked on the subgraph vertices, as are Bob's conclusions (s, m_s).

If we can split the 12x4 tetra star into 3 4x4 OT graphs, then we have a natural strategy: pick one of them consistent with Alice's hand and announce it. During protocol design, to find a first subgraph, start at a node (e.g. 31) and explore (from 0 and 2) how to extend it to an OT graph. The exploration is small. Even when there may be alternative options, there are few, and we end up with what is essentially an isomorphic version of the Tetrahedral OT protocol. Fig. 14 displays three such subgraphs, colored red (X-connections), green (Y-connections), blue (Z-connections).

Another helpful perspective is to consult Alice's directions for Tetrahedral OT as given in Fig. 1. Pick out the cases where she says "Z." There are four. Pick out the outer

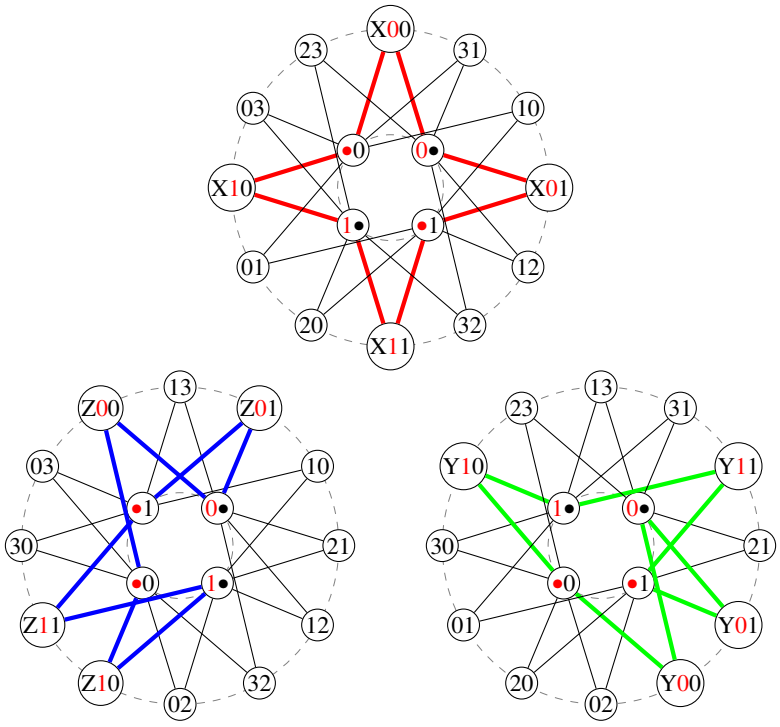


Fig. 13. Bipartite knowledge graph reduced to X/Y/Z conversations, displaying 4x4 OT subgraph.

nodes which are the hands such that she says "Z." The result is precisely the 4x4 OT graph shown in blue in Fig 13.

The typewritten directions in Figs. 1,2 give rise to the needed subgraphs, and if one has started by finding a partition into three OT subgraphs, one can produce typewritten directions. We achieve a generalization of the combinatorial graph theoretic approach in [5] from SKE to OT, specifying when an initial bipartite graph can potentially sustain an OT protocol: when it can be decomposed by partitioning into subgraph(s) containing the OT star via discussions. If it cannot be decomposed, there is no point in looking further.

8 Red-Black OT: an Inferior Approach

An alternative protocol achieves 12OT with a 2/3 rate. It bears similarity to the Tetrahedral OT (which always achieves one OT per deal) and is based on rejection sampling while still using skew-edge notions. Specifically, four of six hands dealt to Alice offer successful completion, while the other two cases must be tossed aside for a retry.

It doesn't directly offer a path toward somehow capitalizing on the throwaway attempts in order to achieve the Tetrahedral-guaranteed (and optimal) rate of 1 OT per S_4 deal.

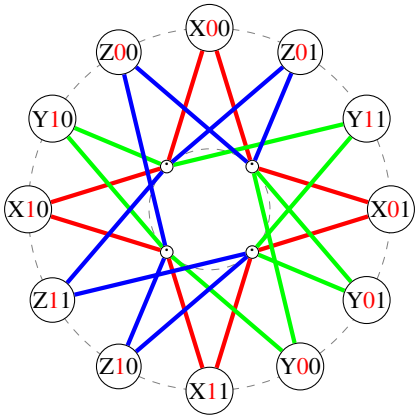


Fig. 14. Three OT subgraphs corresponding to the Tetrahedral OT protocol.

The protocol is intuitively extremely simple in hindsight, hiding in plain sight, almost definitional (apart from its inefficiency), if the four cards are relabeled. We take two cards as red, corresponding to a "'left" channel ($s = 0$), and two cards as black, corresponding to a "right" channel ($s = 1$). Each card has a single bit on it. Equivalently, this is just a set of four distinct cards, {♦, ♥, ♣, ♠}. See Fig. 15.

card	name	L/R	s	color	bitval	suit
0	L0	L	0	red	0	♦
1	L1	L	0	red	1	♦
2	R0	R	1	black	0	♣
3	R1	R	1	black	1	♠

Fig. 15. Convenient labeling of cards 0-3 as L0-L1-R0-R1, also with helpful colorings or suits, red=left, black=right.

The protocol succeeds exactly when Alice receives two differently colored cards. The only message is to convey success or rejection. Each party consults a local table to determine the results. Alice basically sorts and inverts bits; Bob takes the "left-right zero-one" label of his card at face value. Fig. 16 gives details.

Using a French deck with four suits (say, take four aces; the ranks don't matter), an everyday implementation with a 2/3 OT rate simply employs the "renamed" versions in Figs. 19,20.

Theorem 8. *(Red-Black OT) Dealing 2 cards to Alice and 1 card to Bob from a fully-shuffled deck of four unique cards and using the Red-Black Protocol in Fig. 16 implements* $\frac{1}{2}$*ROT with a deterministic protocol, secure against semi-honest adversaries.*

1. Randomly sample $\rho \leftarrow S_4$.
2. Deal $(\rho(0), \rho(1))$ to Alice, $\rho(2)$ to Bob.
3. If Alice receives (L0,L1) or (R0,R1), she terminates the protocol.
4. Alice determines m_0, m_1 according to her table.
5. Alice determines s, m_s according to his table.

Fig. 16. Rejection-sampling "Red-Black" protocol with throughput 2/3

left	right	m_0m_1
L0	R0	11
L0	R1	10
L1	R0	01
L1	R1	00

Fig. 17. Alice red-black table.

card	s	m_s	m_0m_1
L0	0	0	0•
L1	0	1	1•
R0	1	0	•0
R1	1	1	•1

Fig. 18. Bob red-black table.

Proof. The transcripts, results and marginal probabilities are few and very easy to check by hand.

8.1 Red-Black OT Graph Theory Approach

The bipartite knowledge graph for the Red-Black OT protocol is instructive. Prior analysis of SKE and the Two Sheriff's Problem, and the mathematical machinery and conclusions around it, generally sought applications where success is guaranteed – a proper one-time-pad secret is established (SKE) or uncertainty about a counterfactual remains (Two Sheriffs). Here, we weaken the classifications to support Las Vegas attempts which declare failure some fraction of the time, but when they declare success, they meet the success criteria.

First off, the bipartite knowledge graph for a $(2, 1; 1)$ deal remains the same as Fig. 12. The Red-Black OT-Alice rejects any hand of the from {L0,L1} or {R0,R1}. In plain 0-3 indexing, these are the $\{0, 1\}$ and $\{2, 3\}$ hands. They are dealt $1/3$ of the time. Fig. 21 shows the results.

Secondly, on inspection, we can find two embedded OT stars in the overall graph after the rejections. See Fig. 22.

left	right	m_0m_1
♦	♣	11
♦	♠	10
♥	♣	01
♥	♠	00

Fig. 19. Alice red-black table for suits.

card	s	m_s	m_0m_1
♦	0	0	0•
♥	0	1	1•
♣	1	0	•0
♠	1	1	•1

Fig. 20. Bob red-black table for suits.

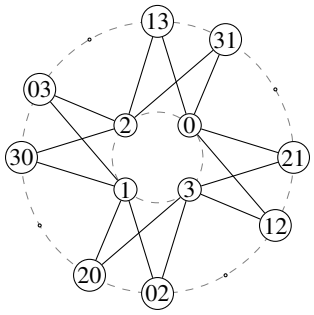


Fig. 21. Red-Black OT bipartite knowledge graph, rejecting some deals.

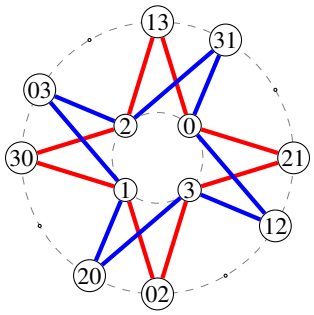


Fig. 22. Red-Black OT, showing OT Star subgraphs.

Finally, disregarding ordering of Alice's hand, these subgraphs collapse to a simple OT star. See Fig. 23 for the cards dealt and Fig. 24 for the values obtained by OT-Alice and OT-Bob in the Red-Black OT protocol.

9 S_n and the 52-Card French Deck

We have seen that S_4 has a 12OT capacity of 1 with deterministic actions and guaranteed throughput. What can be said about larger decks? What about the customary French Deck of 52 cards, namely S_{52}? There is nothing particularly magical about suits and facecards, but they are convenient for describing one approach.

The simplest generalization is to run tetrahedral protocols at the same time. For n a multiple of 4, deal $(n/2, n/4; n/4)$ and consider it an attempt to run $n/4$ executions of Tetrahedral OT.

Let's take $n = 13$ to start, for concreteness. With a French deck, each card rank determines a set of four cards. The aces are one set. The twos are another set. And so forth.

In general, we can assign four suits arbitrarily to larger decks, with non-multiples of 4 being relatively easy exceptions to handle. Suits can just be taken as a card id mod 4, for example. Suits are just names, ♣ = 0, ♦ = 1, ♥ = 2, ♠ = 3.

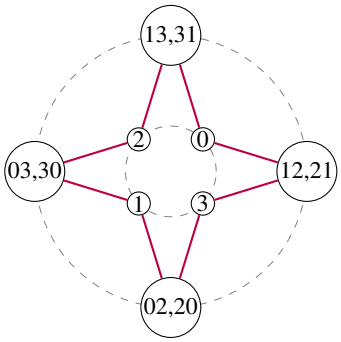


Fig. 23. Red-Black OT hands, order-independent.

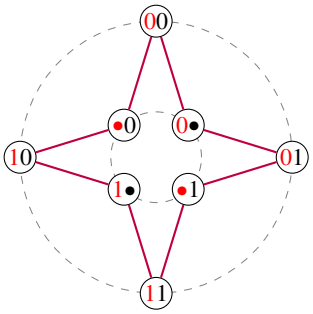


Fig. 24. Red-Black OT results.

The "lucky" case of establishing 13 instances is, naturally, exceptionally rare. A natural optimization is to capitalize on occurrences of $(1, 2; 1)$ deals (as a reversed 12OT). Even with this optimization, fewer than $1/1000$ of deals partition into 13 successes.

Rejection sampling helps. Let $N_A(D, i)$ be the number of cards of suit i Alice received on deal D. Similarly: $N_B(D, i)$ for Bob. We are interested in the cases i where $N_A(D, i) = 2$ and $N_B(D, i) = 1$, or where $N_A(D, i) = 1$ and $N_B(D, i) = 2$. Let $G(D)$ be the set of such i.

Alice and Bob calculate $G(D)$, then run the Tetrahedral OT protocol on each $i \in G(D)$. First, Alice announces $A_2 = \{i | N_A(D, i) = 2\}$ and $A_1 = \{i | N_A(D, i) = 1\}$. Bob calculates $B_2 = \{i | N_B(D, i) = 2\}$ and $B_1 = \{i | N_B(D, i) = 1\}$. Bob announces $G(D) = B_1 \cap A_2 \cup B_2 \cap A_1$.

For $n = 52$ cards, $\mathbb{E}[G(D)] = \frac{81289}{20825} \approx 3.903$, and for n in general, $\mathbb{E}[G(D)] = \theta(n)$.

As a rule of thumb, a standard deck can provide roughly 4 oblivious transfers per shuffle.

(Aside: We also show in further work that a nonstandard deck built from multiple ordinary decks can indeed reach full linear capacity of $n/4$ 12OT per shuffle. Obtaining 13 oblivious transfers per 52-shuffle is feasible with an investment in commercial decks of about one lunch out. But this work focuses on simple S_n permutations of a deck of unique cards.)

Concretely and pragmatically, this means two ordinary persons can establish a baseline of 128 OTs in around 33 shuffles of a standard 52-card deck. These 12OT results can be fed into automated OT-generators and expanded to as many peer-to-peer private computations as they desire. [4, 21] It is not hard to imagine a broader architecture built upon initial peer-to-peer shuffling and post-quantum one-way functions for 2PC and MPC resource expansion.

10 Conclusion

The Tetrahedral OT is the first full-shuffle unique-card protocol to implement $\frac{1}{2}\texttt{ROT}$ and $\binom{2}{1}\texttt{OT}$ securely against honest-but-curious adversaries, showing that arbitrary multiparty secure computations can be implemented with a deck of four ordinary cards.

A distinctively stronger notion of tenancy (results that depend on which party holds which item) is developed to handle the needs of OT going beyond SKE. The narrowing stages of a protocol, in which a loosely structured common knowledge situation is reduced to a structured OT case without violating secrecy of the three essential values (m_0, m_1, s), pursues elegant trifold properties of the tetrahedron and has deeper connections to combinatorial graph theory analysis of SKE (and now, of OT). The graph theory aspects open up avenues for developing MPC from more complicated joint distributions.

This work presents a deterministic table-lookup guaranteed-throughput of 1 OT per invocation and, for comparison, a weaker rejection-sampling solution producing OT 2/3 of the time. Both are simple enough for humans to execute.

Acknowledgements. The author would like to thank Anderson Nascimento, Luis Brandão, Claude Crépeau, Yair Frankel, Stuart Haber, Jasleen Malvai, Peter Winkler, Rebecca Wright.

References

1. Ahlswede, R., Csiszar, I.: On oblivious transfer capacity. In: 2007 IEEE International Symposium on Information Theory. pp. 2061–2064 (2007). https://doi.org/10.1109/ISIT.2007.4557524
2. Asharov, G., Lindell, Y., Schneider, T., Zohner, M.: More efficient oblivious transfer extensions. Journal of Cryptology **30**(3), 805–858 (Jul 2017). https://doi.org/10.1007/s00145-016-9236-6
3. Beaver, D.: Precomputing oblivious transfer. In: Coppersmith, D. (ed.) CRYPTO'95. LNCS, vol. 963, pp. 97–109. Springer, Berlin, Heidelberg (Aug 1995). https://doi.org/10.1007/3-540-44750-4_8
4. Beaver, D.: Correlated pseudorandomness and the complexity of private computations. In: 28th ACM STOC. pp. 479–488. ACM Press (May 1996). https://doi.org/10.1145/237814.237996
5. Beaver, D., Haber, S., Winkler, P.: On the isolation of a common secret. In: Graham, R.L., Nesetril, J., Butler, S. (eds.) The Mathematics of Paul Erdős II, pp. 21–38. Springer (2013). https://doi.org/10.1007/978-1-4614-7254-4_3, https://doi.org/10.1007/978-1-4614-7254-4_3
6. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: 20th ACM STOC. pp. 1–10. ACM Press (May 1988). https://doi.org/10.1145/62212.62213
7. den Boer, B.: More efficient match-making and satisfiability: The five card trick. In: Quisquater, J.J., Vandewalle, J. (eds.) EUROCRYPT'89. LNCS, vol. 434, pp. 208–217. Springer, Berlin, Heidelberg (Apr 1990). https://doi.org/10.1007/3-540-46885-4_23

8. Brassard, G., Crépeau, C., Wolf, S.: Oblivious transfers and privacy amplification. Journal of Cryptology **16**(4), 219–237 (Sep 2003). https://doi.org/10.1007/s00145-002-0146-4
9. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: 20th ACM STOC. pp. 11–19. ACM Press (May 1988). https://doi.org/10.1145/62212.62214
10. Chaum, D., Damgård, I., van de Graaf, J.: Multiparty computations ensuring privacy of each party's input and correctness of the result. In: Pomerance, C. (ed.) CRYPTO'87. LNCS, vol. 293, pp. 87–119. Springer, Berlin, Heidelberg (Aug 1988). https://doi.org/10.1007/3-540-48184-2_7
11. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: 29th FOCS. pp. 42–52. IEEE Computer Society Press (Oct 1988). https://doi.org/10.1109/SFCS.1988.21920
12. Crépeau, C., Kilian, J.: Discreet solitary games. In: Stinson, D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 319–330. Springer, Berlin, Heidelberg (Aug 1994). https://doi.org/10.1007/3-540-48329-2_27
13. Crépeau, C., Santha, M.: On the reversibility of oblivious transfer. In: Davies, D.W. (ed.) EUROCRYPT'91. LNCS, vol. 547, pp. 106–113. Springer, Berlin, Heidelberg (Apr 1991). https://doi.org/10.1007/3-540-46416-6_9
14. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Communications of the ACM **28**(6), 637–647 (1985). https://doi.org/10.1145/3812.3818, https://dl.acm.org/doi/10.1145/3812.3818
15. Fischer, M.J., Paterson, M.S., Rackoff, C.: Secret bit transmission using a random deal of cards. In: Feigenbaum, J., Merritt, M. (eds.) Distributed Computing and Cryptography: Proceedings of the DIMACS Workshop held in Princeton, NJ. pp. 173–182. American Mathematical Society, Providence, RI (1989)
16. Fischer, M.J., Wright, R.N.: Bounds on secret key exchange using a random deal of cards. Journal of Cryptology **9**(2), 71–99 (Mar 1996). https://doi.org/10.1007/BF00190803
17. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th ACM STOC. pp. 218–229. ACM Press (May 1987). https://doi.org/10.1145/28395.28420
18. Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information. In: 14th ACM STOC. pp. 365–377. ACM Press (May 1982). https://doi.org/10.1145/800070.802212
19. Honda, Y., Shinagawa, K.: Efficient card-based protocols with a standard deck of playing cards using partial opening. In: Shikata, J., Kuzuno, H. (eds.) IWSEC 23. LNCS, vol. 14128, pp. 85–100. Springer, Cham (Aug 2023). https://doi.org/10.1007/978-981-97-7737-2_5
20. Imai, H., Morozov, K., A. Nascimento, A.C.: On the oblivious transfer capacity of the erasure channel. In: 2006 IEEE International Symposium on Information Theory. pp. 1428–1431 (2006). https://doi.org/10.1109/ISIT.2006.262082
21. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer, Berlin, Heidelberg (Aug 2003). https://doi.org/10.1007/978-3-540-45146-4_9
22. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A., Wullschleger, J.: Constant-rate oblivious transfer from noisy channels. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 667–684. Springer, Berlin, Heidelberg (Aug 2011). https://doi.org/10.1007/978-3-642-22792-9_38
23. Kastner, J., Koch, A., Walzer, S., Miyahara, D., ichi Hayashi, Y., Mizuki, T., Sone, H.: The minimum number of cards in practical card-based protocols. In: Takagi, T., Peyrin, T. (eds.)

ASIACRYPT 2017, Part III. LNCS, vol. 10626, pp. 126–155. Springer, Cham (Dec 2017). https://doi.org/10.1007/978-3-319-70700-6_5
24. Kilian, J.: Founding cryptography on oblivious transfer. In: 20th ACM STOC. pp. 20–31. ACM Press (May 1988). https://doi.org/10.1145/62212.62215
25. Koch, A., Schrempp, M., Kirsten, M.: Card-based cryptography meets formal verification. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 488–517. Springer, Cham (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_18
26. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE transactions on information theory **39**(3), 733–742 (1993)
27. Mizuki, T., Kumamoto, M., Sone, H.: The five-card trick can be done with four cards. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 598–606. Springer, Berlin, Heidelberg (Dec 2012). https://doi.org/10.1007/978-3-642-34961-4_36
28. Nakai, T., Iwanari, K., Ono, T., Abe, Y., Watanabe, Y., Iwamoto, M.: Card-based cryptography with a standard deck of cards, revisited: Efficient protocols in the private model. New Generation Computing **42**(3), 345–358 (2024). https://doi.org/10.1007/s00354-024-00269-y, https://doi.org/10.1007/s00354-024-00269-y
29. Nakai, T., Tokushige, Y., Misawa, Y., Iwamoto, M., Ohta, K.: Efficient card-based cryptographic protocols for millionaires' problem utilizing private permutations. In: Foresti, S., Persiano, G. (eds.) CANS 16. LNCS, vol. 10052, pp. 500–517. Springer, Cham (Nov 2016). https://doi.org/10.1007/978-3-319-48965-0_30
30. Nascimento, A.C., Winter, A.: On the oblivious-transfer capacity of noisy resources. IEEE Transactions on Information Theory **54**(6), 2572–2581 (2008). https://doi.org/10.1109/TIT.2008.921856
31. Ono, T., Shinagawa, K., Nakai, T., Watanabe, Y., Iwamoto, M.: Single-shuffle card-based protocols with six cards per gate. In: Seo, H., Kim, S. (eds.) ICISC 23, Part II. LNCS, vol. 14562, pp. 157–169. Springer, Singapore (Nov / Dec 2023). https://doi.org/10.1007/978-981-97-1238-0_9
32. Pinto, A.C.B., Dowsley, R., Morozov, K., Nascimento, A.C.A.: Achieving oblivious transfer capacity of generalized erasure channels in the malicious model. Cryptology ePrint Archive, Report 2009/570 (2009), https://eprint.iacr.org/2009/570
33. Rabin, M.O.: How to exchange secrets with oblivious transfer. Cryptology ePrint Archive, Report 2005/187 (2005), https://eprint.iacr.org/2005/187
34. Schneier, B.: Solitaire, pp. 2471–2471. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-030-71522-9-479, https://doi.org/10.1007/978-3-030-71522-9-479
35. Shamir, A., Rivest, R.L., Adleman, L.M.: Mental Poker, pp. 37–43. Springer US, Boston, MA (1981). https://doi.org/10.1007/978-1-4684-6686-7-5, https://doi.org/10.1007/978-1-4684-6686-7-5
36. Sugimoto, K., Nakai, T., Watanabe, Y., Iwamoto, M.: The two sheriffs problem: Cryptographic formalization and generalization. In: Wu, W., Guo, J. (eds.) Combinatorial Optimization and Applications. pp. 512–523. Springer Nature Switzerland, Cham (2024), 10.1007/978-3-031-49611-0-37
37. Wiesner, S.: Conjugate coding. ACM Sigact News **78** (1983)
38. Winkler, P.: Cryptologic techniques in bidding and defense. In: Bridge Magazine (1981)
39. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 222–232. Springer, Berlin, Heidelberg (May / Jun 2006). https://doi.org/10.1007/11761679_14
40. Wullschleger, J.: Oblivious-transfer amplification. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 555–572. Springer, Berlin, Heidelberg (May 2007). https://doi.org/10.1007/978-3-540-72540-4_32

41. Wullschleger, J.: Oblivious transfer from weak noisy channels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 332–349. Springer, Berlin, Heidelberg (Mar 2009). https://doi.org/10.1007/978-3-642-00457-5_20
42. Yao, A.C.C.: Protocols for secure computations (extended abstract). In: 23rd FOCS. pp. 160–164. IEEE Computer Society Press (Nov 1982). https://doi.org/10.1109/SFCS.1982.38

A Appendix: 4-Card OT with Ordinary Suits

The instructions for the Tetrahedral Protocol are specified here using French deck suits instead of integers (as was done in Fig.1 and Fig.2). Thus, for example, when Alice is dealt ♠♥ and Bob is dealt ♣, Alice utters Y and records 00, Bob hears Y and records 0•.

A	♣	♦	♥	♠
♣	·	Z 11	X 11	Y 10
♦	Y 11	·	Y 01	X 00
♥	Z 10	X 01	·	Z 00
♠	X 10	Z 01	Y 00	·

Fig. 25. Tetrahedral Alice for hand $(\rho(0),\rho(1))$, giving message M and bits m_0, m_1.

B	♣	♦	♥	♠
X	0•	1•	•0	•1
Y	0•	•0	1•	•1
Z	0•	•0	•1	1•

Fig. 26. Tetrahedral Bob for incoming message $M \in \{X,Y,Z\}$ with hand $\rho(2)$, giving outputs y_0, y_1.