Cyberdice
(Transcript of Discussion)

Frank Stajano

University of Cambridge

Session 3 Talk 5

The game itself is basically a very simple gambling game where you have people round the table with dice, and everyone has put some money on the table to play, the same amount for everybody. They've rolled the dice, and the one who gets the highest dice roll takes all the money that was on the table. (Imagine for the moment that nobody rolls the same value on the dice: you have dice with a very high number of sides so it's very unlikely that two people get the same number.) So the game is simplicity itself, each player rolls dice, winner takes all.

But we are doing that in cyberspace and the 'cyber' part means that there is no table to put the money on, or roll the dice on: all you see is that you have some network card out of which bits come, and into which you put bits, and all you hear about the other people is that bits come out of your network card. You don't know who they are, you don't know even if they are there, they could all be 'sock-puppets' of someone else. And you have to deal with the issue of rolling dice fairly, and exchanging money, where all you know is these bits that come out of your network card.

We've been talking a lot about modelling the adversary, and here, basically the adversary can do anything that you can do on bit strings. The network is not secure, this is essentially Dolev-Yao at full power. And then, on top of that, everyone else who is playing with you may be a crook, for all you know, because you don't know who they are. And also they may disobey the rules in the most inconvenient way, not just by doing something other than what the protocol says, but also by stopping responding when they're supposed to respond.

Tuomas Aura: So they could be colluding?

Reply: They could be colluding, yes, in fact everybody could be colluding against *you*. And the point is that you don't know if other players are in fact the same player, with different aliases for the same player.

These are the peers of the peer-to-peer situation and any one of them can become the dealer if they like. It's something you decide, you wake up one morning and you decide "I want to make some money, why don't I offer a game of Cyberdice. I'm offering a game with these parameters. If you want to play with me then these are the rules."

The dealer chooses the maximum number of players and if you want to play you must put up perhaps £5 as a player, and he says I will take up to 20 people which means the maximum win that you can make in this game is £100. Up

[Authors' final version as submitted to Springer] (rev. 96)
In B. Christianson et al. (Eds.), *Proc. Security Protocols Workshop 2008*, © Springer LNCS.

front he is going to put up the £100 in escrow with some issuer that he then announces. In so far as you believe the reputation of this issuer that he has chosen, then you know that if you win that game you can get back the money that you have won, up to £100 if 20 people play. Of course if only 7 people play then you can only collect £35. But you know that he has deposited £100 with the issuer, and he can't renege on the fact that he will pay at the end of the game.

Bruce Christianson: Deposit is the same as placing into escrow?

Reply: Deposit is the same as paying into escrow, yes. He chooses acceptable issuers for the players to use in the sense that not everybody trusts all issuers (and so the dealer himself may not trust some issuers that the players may like) to then pay up when it's time for him to collect the fee.

Matt Blaze: Does the game end for everyone at the same time?

Reply: I'll get back to that, the game ends when the winner is designated, and then at that point you can claim your money if you were the winner, or you have lost your money if you were another player, but there are some subtleties there too.

Tuomas Aura: So we have sessions?

Reply: We have sessions, yes. The dealer competes against other dealers on the fee that he charges to play his game. The issuer also charges a fee: there's a fee charged by the issuer, and there's a fee charged by the dealer. Because the dealer collects the fee from every player, and pays out whatever money was on the table, the dealer always makes a profit. His profit is the total of the fees paid by every player, and is independent of the outcome of the game. The dealer doesn't care who wins, he always makes the same amount from the fees that players pay him. The gamblers are players who bite to the lure offered by a dealer: they accept the invitation to gamble and they bid by going to an issuer of their choosing (chosen among the set of those approved by the dealer of that game) and they say: let me put into escrow this £5; of course I'll pay you the fee, in fact I put into escrow £5 plus ϵ, where ϵ is this extra fee that is charged by the dealer, and I get back a bit string that proves that I have put this money in escrow. I can put it on the table, and show how this can then be redeemed by conceptually the winner of the game, but practically the dealer because the winner of the game is in fact collecting money from the dealer's issuer, if you are still with me. Are you still with me? Yes.

So now we get back to something that Matt mentioned: when does the game finish? Does it finish at the same time for everybody? Since there is a maximum number of players that the dealer accepts, there can be many more players wanting to play than this number: but the dealer at some point will select who gets to play (I'll get into greater detail in a moment). People who did put money in escrow but were not selected to play (i.e. get to the next stage) then get their money back from their own issuer, and they have to prove to the issuer that they were not admitted into that game. Or of course if they can prove that the game was fraudulent then they can also get their money back. And unlike these other two types of principals (dealers and issuers) who will always make a small

profit, the gamblers may win more than they put in, or they may lose everything they put in. And of course, as expected value, on average they will always lose, and so you would be excused for thinking: "why would anybody play this game if they always lose?". First of all, this is true of all gambling games, more or less. And secondly there is a non-obvious, subtle and interesting answer to that, which was given by some guy who won a Nobel prize for figuring this out.[1] You are given a choice: "would you rather get 1p or a 1 in 10 chance of getting 10p?" And, "would you rather get 10p or a 1 in 10 chance of getting £1?" and so on. All these things are to be considered independently of each other. You will typically see that people say: "I can do nothing with 1p, just give me the chance of getting 10p and at least it will be worth my while". But by the time you get to, "would you rather have £10,000 or a 1 in 10 chance of getting £100,000", it's: "give me the £10,000 right now". So, depending on how rich you are, there's a switchover point somewhere in the middle, and your wealth tells something about where you put the breakout point. Anyway, this explains that if the bet is small enough it may be worth your while, psychologically, to go for the gamble instead of just holding onto the 1p. I just put up this slide so you don't worry for the rest of the talk, wondering why would anybody play this game.

James Malcolm: Maybe this is a 0.1 version of the protocol, but it seems to me that at the moment the issuer is implicated in this illegal gambling business, because he's having to look at the log that says who should be paid, which is gambling specific, isn't it?

Reply: No. Well, what I am trying carefully to avoid is having the issuers implicated in that, and the way I claim they are not implicated is that they just make a contract with the player saying, in exchange for the fee that you give me I'll hold onto this money and I will pay it back to whoever gives me a bit string with these properties, and these properties are that some signatures match, and this and that, and it points at some guy that they can prove has a certain public key, and so on, but they're not involved in any of the gambling, they're just honouring a contract about properties of a bit string: whoever presents a bit string with those properties, they will give them back the money that you are depositing now.

James Malcolm: And the properties are not gambling specific?

Reply: The properties are not gambling specific.

Matt Blaze: So it's plausible that that protocol is useful for just general money transfer between people?

Reply: Well, that is the intention, in fact I would love to make this function of the issuer as detached as possible from the Cyberdice game, although as you will see in what I'm presenting now, it is fairly entangled in it in that the contracts have to know a lot about how the Cyberdice game works. But ideally I would like to have the issuers in a position where all they do is just have a very formally defined and detached contract with customers about properties of bit strings where, as a service, they say: you pay me money and give me a bit string with certain properties, and I promise I will pay that back to anybody

[1] Harry M. Markowitz, Nobel Prize in Economics, 1990.

who presents another bit string with some other properties, and I don't want to know about gambling, because gambling is wicked.

Bruce Christianson: So this could be used for drug dealing and arms running as well as gambling.

Mark Lomas: You appear to be suggesting that gambling is worse than breaching the know-your-customer part of the Anti-Money-Laundering regulations.

Reply: I do; which you think is worse depends on jurisdiction, I guess.

What happens is that each player rolls the dice and gives the (allegedly) random number so that you have a contributory strategy where everyone supplies part of the random number that is selected. You don't want to have someone else choosing your random number for you! This randomness is stirred up, or hashed, and used to decide who will win. The key technical point is that you must commit to your own randomness before you get to see other people's randomness.

So here are the slides with the protocol...

Right, so I guess the bit that isn't solved in those protocols that I've presented there is how to ensure that players actually reveal the values they commit to. The issue here is that gamblers give you the hash of their dice roll and then they don't tell you what it is. When everybody has given their own commit, then you say, OK, reveal what it was, then we hash them all together, and then the number that's closest to that from below will be the winner. But, what if some people don't actually answer? What if some people give you the commitment and then they don't give you the number when they're asked to reveal? In that case you can't compute the final value.

Virgil Gligor: Once they commit to a value, how do they not give you the numbers?

Tuomas Aura: You choose a random number, let's say 73, you give me the hash of 73; I can't work out 73 from that and I say: "so, Virgil, what was your number that gave you this hash?" and you just go quiet. And I don't know who you are, I can't go and beat you up because I just have a public key, so of course you lose your money, but you denied service for everybody else.

Mark Lomas: It's easier to understand why if you think the last person to give a commitment is the only one who actually has something to gain. If you're going around the loop, if you don't know what's going to happen afterwards, you might as well give your commitment, but the last person has an incentive to muck up the whole thing.

Matthew Johnson: Because the last person can change the outcome by deciding whether or not to send theirs in, and if you have a sufficient number of people who do this, then they can essentially make sure one of them wins eventually by withholding their value.

Reply: Exactly this. You have a problem because everybody needs to reveal the value they committed to in order for us to determine a winner, but then you are at the mercy of people not continuing, and then you can't designate a winner. If you say "we will only continue with those who did reveal" then the winner changes depending on whether people participate or don't participate;

and, as Mark pointed out, the last person to reveal would know whether, by revealing, they win. I mean, they will know who wins whether they reveal or whether they don't reveal, and they have pointers to two people, one of them could be them, but it could be just two other people, and they can say, OK, I can influence the outcome and make you win, or I can make *you* win, and how about we split if I make you win? Something like that. Or they could arrange to have even more people playing last together and then having all the possible combinations. Actually it's not even necessary to have all possible combinations, just interesting to be able to influence the outcome and point at the people you like.

So we have a problem if we want to use this system because we would like everybody who does commit to be forced to also reveal. But we cannot enforce the atomicity of this, which means that there is an advantage for the last gambler. This is something that is difficult to fix.

One solution that was suggested by Mark by email, if I remember correctly, was to say "if someone doesn't reveal then they have to pay a fine", but on second thought this won't work because if by cheating in this way you could win the whole game, then the fine would have to be a sufficient deterrent for you not to do that, even in case you win the whole game, which would mean you would have to escrow enough money to be fined for the whole value of the game, which you might not be willing to do. You might like to gamble £5 on the game, but you might not want to put up £100 just to play the £5. More so if there are a hundred players or a thousand players allowed by the dealer, instead of just 20.

Tuomas Aura: Even that solution, although it sounds like it would work in theory, has problems if you think of when is the deadline for you to reveal something, because if someone can push you over that deadline, or just pretend not to receive, everyone else says, we haven't heard from you, you keep resending, and they say, we haven't heard from you, and the deadline passes, and now you owe them money.

Reply: That's absolutely correct. In this particular set of arrangements that we have taken, this is taken care of by the fact that the issuers are resistant to denial of service. And so, if you send a message to your issuer, then the assumptions under which we play guarantee that this will be blogged by the issuer, so you have a proof that you did submit by that time. But otherwise in general that would be a valid point: if you could be stopped from sending your message then you would lose all, you would be fined for the whole fee of the game. So we don't like this one.

What about removing the commitment phase, just making it atomic, by making everyone announce the dice roll so there aren't two phases here. Well obviously that can't work because then the last guy sees everyone's dice roll and then he could decide what to roll on his own. So another suggestion that came up, I think this was Richard's idea, was to use a kind of time delay mechanism where you obscure your own roll with some encryption that could be broken if you spent enough time on it, but can't during the normal run of the game. But of course that also isn't very desirable because the capabilities of people for

breaking encryption vary by many orders of magnitude so you would never be sure that nobody during that game duration can do that, especially if it needs to be sufficiently breakable that if someone drops out you can then reveal it later.

So what we did instead was to change the way in which the randomness is stirred up to select a winner from the dice rolls. If all these issuers have to sign the messages that they receive anyway, then by signing they introduce some randomness with their own signatures; so why don't we introduce that in the mix as well? The message where all the dice rolls have been revealed is passed around by the dealer to all the issuers involved, which may be many fewer than the players, because several players may have chosen the same issuer, and then each of them signs it, and the result of this is then hashed to produce a target value to designate a winner.

Matt Blaze: It seems to me that you're living in a bit of a state of sin here, beyond the gambling, in that you are depending on a property of signatures that I'm not sure I understand that they have. It seems intuitive that signatures have some sort of unpredictable randomness property to them, but I've never understood that to be a necessary property of signatures.

Reply: Yes, well, as we have written in the position paper, we don't really understand it either, but we believe it's plausible enough, and if you throw some hashes at it, then we think it would work. But I take your point, and I think we just wrote it explicitly in the paper. I'll just quote myself...

Matt Blaze: My excuse is that I haven't read the paper.

Reply: You're not supposed to, but I'll just prove that we thought of that: *"The game can be seen to be fair, in that it is well-known (albeit possibly hard to prove) that signatures made with high quality cryptographic primitives are random. If this isn't believed to be true of signatures in general, then placing their values into a canonical order and then calculating a cryptographic hash of this concatenation will provide an 'even more random' value."*

Michael Roe: Are you assuming the signature is deterministic by RSA and non-deterministic by PSS? The issuers might try and cheat if they could do so undetectably.

Reply: We want the signatures to be deterministic for exactly that reason. We want to make sure that once you are given something to sign, there's only one thing that could come out of it.

George Danezis: But how does that go hand in hand with the fact that you want some randomness in the signatures? I was following this debate saying ah, you know, it's all right because secure signature schemes have to be non-deterministic. And now you say, no, we want them to be deterministic?

Reply: Well, random in the sense that you couldn't predict ahead where it's going to point at, but yes.

George Danezis: Unpredictability if you don't know the secret key, effectively?

Reply: Yes.

Bruce Christianson: The signatures don't have to be random, they just have to be unpredictable.

Virgil Gligor: But you can add the randomness to them, you can make signatures sufficiently random artificially, like MACs.

Reply: But we want to be really careful that we are not allowing the signers to make things point the way they want, they shouldn't have any option to make something come out.

Richard Clayton: I think that we're going down a rabbit hole here with randomness, because as part of the point of this paper, we tried to dismiss all of the trivial flaws that people normally find in protocols, so as Frank says, we chuck absolutely everything into every message because we don't want you to start looking at this protocol from the point of view of "where does the randomness come from", or the point of view of "can we pretend using this message in this phase of the protocol instead, and that might break it" etc; this isn't what this paper is about. This is about the fact that, because we don't know any theory (we are terribly practical people) if we knew any theory we wouldn't try to do this, because it's impossible. The theory people proved long ago that what we're trying to do is impossible: you can't do a multi-party computation with n people with only one of them being honest, this is a nice theoretical result from the 80s. OK, so we tried to do that. And the other thing is, the theory people know about the property that some of the people go home in the middle (they even gave it a really silly name which I can't even remember now[2]) and they worry about this, and they've written papers about it, full of lots of Greek letters, and you can't understand a word of it, so we're trying to write something simple here. All the theory people suddenly get really excited from this slide, because suddenly we've got n people participating again, at which point it's all possible.

So that's the real point of the paper, it's to draw the attention of this community to the fact that people can go home in the middle of the protocols. Propping up the whole of your paper on Yao's millionaire protocol doesn't work if one of people goes home right at the end of the protocol. And we put some money in here, so people could see that it was important that it didn't work!

Reply: Yes, that's a subtle point. Please don't miss the last bit that Richard said because it really is crucial: in Yao's multi-party computation, at the end one of them knows the result and has to tell the other. What if he doesn't? We try and fix that.

Michael Roe: If the adversary can predict what the secret message was going to be then they could forge signatures, so I think the unpredictability property you want is a natural point of the signature algorithm being a good signature algorithm.

Bruce Christianson: But there's still a danger that the person who signs last might have an advantage, using a signature algorithm?

Reply: Yes, and I am shifting who's last from the players to the issuers, who have some reputation. So the people who are slightly more trustworthy do that, and I'm trying to arrange things so that a single crooked issuer can't rig the game undetectably.

[2] *Independence.*

Tuomas Aura: So basically what you have here is a kind of trusted third party that can compute a one-way function, but it's deterministic, and everyone can verify that it was computed correctly. It's important that it's deterministic because otherwise the issuer can cheat.

Reply: Yes, insofar as you want the thing to be auditable. I trust this guy, because he's done it a hundred times, and he was always fine, but if he could hide his tracks, and do it a hundred times and it looks like it's fine but it isn't, then there would be no point in this reputation game.

Tuomas Aura: But it feels there's a need for different cryptographic properties if you want this function, and let's not talk about signatures, because you're not actually signing them.

Reply: Why not? I am signing something aren't I?

Tuomas Aura: But the property that you need is not the signature.

Reply: Well it needs to be something only that guy can generate and everybody else can verify, that looks like a signature to me.

Matt Blaze: But PSS does include in these properties, because it's randomized.

Tuomas Aura: Yes, so you're saying it has to be deterministic?

Matt Blaze: Right, so which non-randomised signature algorithm is still considered secure?

Tuomas Aura: Maybe for these purposes you do not need a proper signature, you might just use something like plain RSA.

Matt Blaze: Plain RSA with no pattern, or with deterministic pattern?

Bruce Christianson: But even with vanilla RSA, I'm still worried that a corrupt issuer might force you into a smaller subgroup by having a modulus of the form pq^2 or something.

Matt Blaze: I'm more worried than ever that you're depending on cryptographic primitives that may not exist.

Matthew Johnson: You're moving the "who does something last", to the issuers, and we have previously discussed what the problem would be with crooked issuers. Can the issuer here not do exactly the same as the wicked user just by refusing to sign things?

Can I ask another point about this? You might not need a complete digital signature, but you can't just use a one-way function per se, because you need to be able to verify that the issuer has done the correct one-way function.

Reply: The issuers are, to some extent, part of the trusted computing base, and always will be: if nothing else because you give them money that they could always not return, so you have to put some trust in the issuers, whatever happens. But I would like to limit this trust to things that will show if they misbehave in the audit log. Some of these things I still can't, for example, the atomicity of some of the transactions, the fact that if I send them some money I want to get the bit string back. If I don't get the bit string back I have no way to prove that I sent them the money, so I am dependent on that.

Matthew Johnson: But that's you trusting your issuer rather than you trusting anybody else's issuer.

Reply: Yes, but insofar as I take part in a game for which the issuers have been announced at the beginning, I can make a decision on not to participate in one because it contains some issuers that I don't trust.

Richard Clayton: First of all, you are told which issuers will be accepted and they do have a long term reputation, so if you don't like them because they're dodgy then you don't have to play. The second thing is that because they make money from the game they will be interested in looking at the long term.

Reply: I see that I am restoring the original intention of the protocols workshop as a place where you get interrupted all the time.

Tuomas Aura: I may be missing something but don't you get a much simpler protocol by letting the issuer commit to a nonce and the issuer reveals the nonce last.

Reply: I guess we are sliding more and more into grounds where the issuer does the gambling.

Richard Clayton: If people are trying to simplify this then I think that it makes the game run in a different way without all the fluffing around that you need in order to make the thing look like the original throw of the dice, which we've kind of forgotten in all of this. We haven't mentioned throwing the dice and choosing the highest number for some time.

Reply: Roger Needham once said, optimisation is the process of taking something that works and turning it into something that almost works but costs less, and so I apologise, I'm going to do one of these now.

The thing that I am going to optimise away is people throwing dice, so we say, if we are using the issuers' signatures to stir the randomness, why bother even with the dice? We can even save all this "doing the commitment" stuff, since ultimately we need to have it signed by all the issuers anyway. Now why does it become something that only *almost* works? It is because I am no longer fully contributory. At the beginning, I wanted everybody to chip in with their bit of randomness to make sure, but here you just have to make sure that you trust the issuers that are involved, and this is why it is slightly dodgy.

What happens then is simply that the dealer announces the game, the properties of the game, the lines of the game, and so on; the gamblers send their stake, which is their proof of having escrowed the money to play; the dealer selects a subset of the gamblers by the deadline; then this selected subset is signed by all the issuers in a pre-determined order; and then this gives a number which points at one of the people in that selected subset, who becomes the winner.

George Danezis: But can the dealer select the subset so as to influence the outcome?

Reply: Well he can't because he doesn't know the outcome of all these signatures that have yet to happen. The dealer selects a subset of the gamblers, so it includes all these commitment strings of the money, takes it all together, signs it, and then hands it over to all the issuers in turn, sign that, now sign that, now sign that, it comes back to him, he says, OK, now let's hash it and reduce modulo k, and we get a number which points at one of them.

That's why we don't need a commitment anymore, because the dealer doesn't know yet what will happen after all these issuer signatures. At that point the winner can go with that lump of stuff to the dealer's issuer and say, look, this proves I am the winner. Actually it only proves that the guy who controls the secret key corresponding to the public key in that slot is the winner, and now I can prove I have that secret key, and then you give me the money. The subprotocol for that, where again there is a jeopardy for the player with respect to the issuer where he could be doing the proof and signing a receipt, and not having got the money yet, and that is unavoidable because of the position the issuer is in. And then there's the usual thing as before, the dealer goes back and collects the money that wasn't actually played, and all that kind of stuff.

Tuomas Aura: Was there any randomness in there?

Reply: Well there is some randomness insofar as each player selects a new ephemeral key pair every time they play, so the fact that dealer is choosing a new key pair for playing makes this a kind of identifier for that game. In fact the public key itself is also a nonce, and if you are arguing that he could choose the same public key as the previous time, well he could also choose the same nonce.

Tuomas Aura: So do they commit to the public key?

Reply: The first time you hear about that public key for the dealer is when he announces the game: he says, and here is my public key.

Tuomas Aura: OK, so is the dealer the only one who has a new public key?

Reply: No, every player, everybody except the issuers always has a new public key every time they play.

Matthew Johnson: And you need that so that the dealer can't be ...

Reply: Recycling games, exactly.

Tuomas Aura: So commit to the public keys, and you again have the problem of does everyone play till the end.

Matthew Johnson: No, because you're actually just using the keys themselves to generate randomness. You don't need them to reveal their private keys, they can start playing whenever they like, and it's fine.

Reply: What's the remaining problem, you have a puzzled face?

Tuomas Aura: It's not showing here the details of the protocols, but at some point there is some order in which people commit to random values, someone will be the last, or maybe someone can just delay till they are the last, so to avoid this you need some kind of commitment phase, and then you then have a problem, who will reveal last?

Reply: Well the point is that if all the randomness you contribute as a player is your public key, then it's going to be very hard for you to rig it up.

Tuomas Aura: But someone is going to sign that.

Richard Clayton: Yes, let's be very clear about this. The threat is that the issuers will cheat. In order to fix the theoretical problem, which is that we can't do this, we give the issuer the property which at the beginning we said we weren't going to give them, and we say, because they have a long-term reputation, we can get away with it. The issuer is trusted to actually do it because of the security

economics of the game: the issuers have big incentives not to cheat in order to win one game.

Bruce Christianson: Because the issuer won't go home.

Reply: So the issuers are the only ones with permanent key pairs, everybody else has ephemeral key pairs, so the reputation hangs on the public keys that are permanent.

Virgil Gligor: So the issuer acts as a certification authority for those keys, and that's a commitment to the keys.

Reply: Yes. When you escrow your money you get back something that's signed with the long-term key of the issuer, which in a sense is a certificate that you have this public key insofar as the game is concerned.

Matt Blaze: Just to clarify the security model, the trust model here is that the issuers will not cheat in ways that they can be caught, not that they will not cheat period.

Reply: If they could cheat in a way that nobody sees from the log, then I'm sure they would.

Bruce Christianson: Yes, but going home is very visible.

Reply: Yes, absolutely. And the point is also that if you believe someone is misbehaving then you can choose not to participate because you will know in advance which issuers are involved, because in the announcements of the game the dealer will say, I'm using this issuer, and you can only use one of these issuers. So if you see that, you think I'll be dealing with these issuers, well, I'll just pass on this one.

Tuomas Aura: I'm still worried about, what determines which players get within that subset, maybe some players will be flooding in at the end.

Reply: We are taking away any chances for the players to mess things up by only giving them one thing to do, to say, I want to play, and I have deposited my money. Do I get selected, I don't know, this depends on the dealer, if I get selected I can't decide not to play anymore because I've already said I'd play, and that's it, which removes most of the screw-ups they could introduce in previous versions.

Virgil Gligor: I want to understand more about the commitment to the keys by the issuer. Two players chose one issuer, and two players chose a different issuer, what does that commitment to the key mean? Do the issuers talk to each other? I get my key signed by you as an issuer, so you are my certification authority, somebody else has a different certification authority whom I don't trust. Does the fact that it's a different issuer make a difference?

Reply: Well it's slightly different from what you say, insofar as you are taking part in a game where various issuers are involved, and you have to, to some extent, trust all these issuers, otherwise you wouldn't take part.

Matthew Johnson: You see the list of issuers before you join because it's published.

Reply: Yes, it's in the game announcement, the dealer says, this is the list of issuers that I will accept for the players.

Virgil Gligor: So that's one of the fundamental assumptions?

Reply: Yes.

Richard Clayton: The trust is not just in their public key, the trust is that they are saying, the dealer has given me £100, and you can collect it. So the trust is very real, and if you don't feel that the St Petersburg Trust Issuing Authority is the right one to use, then you don't want to play this game.

Virgil Gligor: If everyone trusts this group of people this is no longer a decentralized problem.

Reply: Well the trust placed in the issuers is slightly different for the issuer of the dealer, and the issuer of the player. The issuer of the dealer, you have to trust him to actually hand out the prize money, because that's the whole point for you to play. The issuers of the other players you have to trust them to do the signature without rigging it up, they're not going to give you back any money, so it's slightly different, but you still have to trust them.

Virgil Gligor: But there is central trust in this dealer's issuers and this core of issuers.

Reply: Yes, that's the cheating bit.

Virgil Gligor: That's the cheating bit, that's because you haven't been able to solve the original, impossible problem.

Tuomas Aura: You could do the same with nonces again, by letting the issuers commit to nonces, and then once the dealer decides on his nonce, and now you just have the original game, but with a difference since the issuers have to continue to the end of the game by the rules that they're guaranteed to finish it.

Reply: So what advantage did we gain?

Bruce Christianson: I don't think that works because the issuers can dishonestly share their nonces.

Tuomas Aura: No, the issuers can also share their private signature key, or they can act as oracles for whoever wants the key, so it's just as if you wanted to share the nonce.

Bruce Christianson: But if I share my private key with someone ...

Tuomas Aura: No, but you might give someone access to your private key for the purposes of this protocol by acting as an oracle.

Bruce Christianson: But in this protocol they sign in order, so I don't know what I'm going to sign till I get it, so I can't reveal the signature until I'm going to have to anyway.

George Danezis: It depends on how many potential players there are. If there are exactly as many candidate players as there are going to be players playing the game, then the attack that Tuomas describes would work, because you could have a crook issuer that will give you access to their key as an oracle, and then they will be able to choose whether to participate or not depending on what kind of values they would sign.

Bruce Christianson: Maybe I haven't understood the protocol, there's a block that goes round all the issuers, each one signs on top of the other one.

Richard Clayton: There were various schemes with only one signing, and they don't work.

George Danezis: Aha!

Matt Blaze: Perhaps I'm uneasy about this protocol because it seems very complicated and specific to solving two things at once. One is establishing the outcome of the game in a distributed fashion with the appropriate deniability among parties, and the second is settling the payments after the outcome of the game, where the game is a simple guessing game. Well it seems that gamblers have historically solved the establishing the outcome of the game, that is having a secure random number generator, long before computers and distributed computation, by simply relying on a published source of randomness that everyone agrees is unpredictable. For example, the classic numbers game in the United States, and maybe elsewhere, uses to establish the outcome things like horse races, or the lower bits of the closing stock price on the Stock Market, or some other widely published readily agreed on, and hard to influence or predict, number. If you have a source of such numbers does your protocol become simple, does it simply reduce to the settlement part of the problem and is that simple?

Reply: Well I like this comment, I guess it might. I can't answer on my two feet like that, but if we could separate it out and have a way of dealing with the money in cyberspace, and then just use the random number you mentioned as a pointer, reduce modulo K among the people who have played, we would still have most of the issues here: selecting who plays, in which order, so that we are arranging them and so on.

Matt Blaze: Right, maybe it doesn't make it simple well, maybe it does.

Reply: Well yes, because there isn't that much else in this game other than, putting the people in order, and then selecting one. I'd be happy if we found a way of simplifying that, and especially separating the payments out of that.

Matt Blaze: I think the published sources of randomness have a long history in gambling, and there's something poetic if you can employ them here.

Reply: It's nice to separate concerns, and the thing that would be even nicer for me would be to separate as much as possible the action of the issuers from the working of the Cyberdice game protocol itself, so that the issuers offer a service that could be used for many other things as well. It's basically always the same service, you give me some money, I'll give you a bit string, and there are certain conditions.

James Malcolm: I think maybe the problem with Matt's suggestion is, in the Internet everybody has access to the same random number, which is not big enough, and they can collude. In the real world, a bunch of gamblers in Texas cannot collude with a bunch of gamblers in New York, so that the two games use the same random number, I think. Or can they?

Matt Blaze: Yes, they can. For example, if I'm using something that depends on the global economy, or that depends on some likely observed natural phenomena ...

James Malcolm: Yes, it's a matter of choosing enough different such numbers, that's what might be difficult.

Matt Blaze: That's right, these numbers may be in limited supply.

James Malcolm: Exactly.