Date (UTC+1)	Sender	Text	ID
17-05-20 4:09	**Max Krohn**	Nadim, hi! Quick question about verifpal. I can't get simple.vp to verify, it says that basically that Alice can learn the message if she attacks the protocol (which is the point, right?). Is there a bug, am I reading it wrong, or is this all expected behavior? Thanks!	1261871347623505924
17-05-20 4:09	**Nadim Kobeissi**	Give me a sec, just woke up	1261871481920913413
17-05-20 4:10	**Max Krohn**	please say i didn't wake you up	1261871684593881094
17-05-20 4:10	**Nadim Kobeissi**	You didn't ☺	1261871728336285700
17-05-20 4:10	**Max Krohn**	ok, if i did, then go back to sleep, please god!	1261871775505408005
17-05-20 4:11	**Nadim Kobeissi**	You didn't jeez	1261871819977613317
17-05-20 4:11	**Max Krohn**	i basically ran this on mac 0.13.4:	1261871935056760841
17-05-20 4:11	**Max Krohn**	./verifpal verify ./examples/simple.vp	1261871939179733001
17-05-20 4:11	**Max Krohn**	cool software btw!	1261871967394766853
17-05-20 5:13	**Nadim Kobeissi**	Okay I'm at my desk	1261887511913168900
17-05-20 5:13	**Nadim Kobeissi**	Oh yeah sure	1261887593207209988
17-05-20 5:13	**Nadim Kobeissi**	simple.pv is expected to fail dude	1261887613981556741
17-05-20 5:13	**Nadim Kobeissi**	It's not secure	1261887627218780164
17-05-20 5:13	**Nadim Kobeissi**	You can clearly see that a man in the middle is possible on both Alice and Bob	1261887665533788166
17-05-20 5:14	**Nadim Kobeissi**	Did you read the manual?	1261887678934589444
17-05-20 10:21	**Max Krohn**	Ok thanks, I skimmed it.	1261965007232872453
17-05-20 10:26	**Nadim Kobeissi**	I'm very excited you're trying out Verifpal! Please do ask me more questions	1261966223396483083
17-05-20 10:26	**Nadim Kobeissi**	Didn't mean to just throw the manual at you	1261966254925119492
17-05-20 10:26	**Nadim Kobeissi**	Also you can join our Discord	1261966268569133065
17-05-20 10:26	**Nadim Kobeissi**	I don't know if you saw the VSCode extension	1261966376866119684
17-05-20 10:41	**Max Krohn**	I did see that, this is all very cool. OK, I figured out what was wrong with my protocol, i forgot the "?" after SIGNVERIF	1261970177018773508
17-05-20 10:44	**Max Krohn**	As someone who attempted to make a product competing with signal and who failed, I think the extent of my frustrations boils down to this: [gblongterm] versus gblongterm. I'd say, you shouldn't make that assumption, it's crazy! The whole world seems to say, "it's fine, add the brackets, the rest of the math is soooo cool." Oh well! :) Not a knock of verifpal, very cool stuff Nadim!	1261970724794896388
17-05-20 10:44	**Nadim Kobeissi**	Well that's what TOFU is for	1261970897981845508
17-05-20 10:44	**Nadim Kobeissi**	Can I see the protocol you're modeling?	1261970941623570437
17-05-20 11:05	**Max Krohn**	Loving verifpal, amazing stuff!	1261976123661070341

17-05-20 11:05	**Max Krohn**	Signal isn't TOFU, it's like Trust-on-every-device-addition-or-revmoal	1261976214652280836
17-05-20 11:07	**Max Krohn**	https://t.co/W2l8eVsv21	1261976615636123654
17-05-20 11:09	**Max Krohn**	how can i assert they call get the same session key?	1261977201488146442
17-05-20 11:12	**Nadim Kobeissi**	Very interesting question	1261977850879631364
17-05-20 11:12	**Nadim Kobeissi**	You want to show in the model that all principals necessarily agree on the same session key?	1261977962741628940
17-05-20 11:13	**Max Krohn**	Right, like i'd want it in my queries, tho I could of course whip up an zero-knowledge proof to do it	1261978110544826372
17-05-20 11:13	**Max Krohn**	(it's not that big a deal, obvious AEAD_DEC doesn't fail, so it's gotta be what went in)	1261978223237312516
17-05-20 11:15	**Nadim Kobeissi**	This is an excellent suggestion	1261978679258894340
17-05-20 11:15	**Nadim Kobeissi**	Let me think about this and get back to you in a few ho it’s	1261978705901096965
17-05-20 11:15	**Nadim Kobeissi**	Hours	1261978713006243844
17-05-20 11:16	**Max Krohn**	thanks Nadim, not a big deal either way. really enjoyed playing with Verifpal, you've done an amazing job on it	1261978823102521351
17-05-20 12:13	**Nadim Kobeissi**	More to come!	1261993343485128708
17-05-20 12:14	**Nadim Kobeissi**	Yes I think you can infer that they agreed on the same shared secrets if checked primitives don’t fail	1261993532736372741
17-05-20 20:38	**Max Krohn**	One small item of feedback, I think this should cause a warning or fail:	1262120254232281094
17-05-20 20:38	**Max Krohn**	_ = SIGNVERIF(ga, gea, siga)	1262120262734090247
17-05-20 20:38	**Max Krohn**	(without the question mark, since otherwise it's a void statement, right?)	1262120345277997061
17-05-20 20:38	**Max Krohn**	(though of course I could be wrong; this was my only bug, and otherwise, everything "just worked")	1262120451783999493
18-05-20 6:15	**Nadim Kobeissi**	Nah, question mark should be necessary	1262265413284638724
18-05-20 6:15	**Nadim Kobeissi**	If you guys end up using Verifpal at Keybase or Zoom, it would be nice if I could make a tweet to that effect from the Verifpal account for promotional purposes!	1262265534906843141
18-05-20 10:12	**Max Krohn**	Of course!	1262325266094964740
18-05-20 10:38	**Nadim Kobeissi**	Do you plan on using it anywhere?	1262331734181457925
18-05-20 11:35	**Max Krohn**	We plan on using the protocol I just sent you to secure Zoom meetings. Can I ask you a stupid question? What's wrong with this proposed protocol and why does every insist on DH everywhere (i.e., Noise)? This protocol seems so simple and it has the right security properties.	1262345982068604933
18-05-20 11:35	**Max Krohn**	every -> everyone	1262346118668713994
18-05-20 11:35	**Nadim Kobeissi**	https://t.co/OCjmjQYpyb	1262346136926466052

18-05-20 11:35	**Nadim Kobeissi**	To be clear, it's this exact one?	1262346136121217028
18-05-20 11:36	**Max Krohn**	yeah, this exact one (but for N parties not 3, where Alice is the "leader")	1262346209949294598
18-05-20 11:36	**Nadim Kobeissi**	(btw this is obviously incredible, it would be amazing if we were able to at one point say that Zoom's new e2e was prototyped with the help of Verifpal)	1262346396981768196
18-05-20 11:36	**Nadim Kobeissi**	Looking at it closely now	1262346437863620614
18-05-20 11:37	**Max Krohn**	(What claims could I actually make BTW? "This protocol is formally verified"?)	1262346664930611205
18-05-20 11:38	**Nadim Kobeissi**	So	1262346910498729988
18-05-20 11:38	**Nadim Kobeissi**	This is a perfectly reasonable protocol	1262346914579787782
18-05-20 11:39	**Nadim Kobeissi**	The reason why people do DHs a lot is because generally speaking, Signal sessions can (and usually do) last weeks and months	1262346995060047876
18-05-20 11:39	**Nadim Kobeissi**	Whereas a Zoom session lasts minutes or hours at most	1262347028320968708
18-05-20 11:39	**Nadim Kobeissi**	So here you're generating ephemerals *per session*	1262347062248648708
18-05-20 11:39	**Nadim Kobeissi**	Which means you have post-compromise security per-session	1262347087859068932
18-05-20 11:39	**Nadim Kobeissi**	Which is fine	1262347094393794566
18-05-20 11:39	**Nadim Kobeissi**	It's perfect for this use case	1262347114463596549
18-05-20 11:39	**Max Krohn**	Ah right, so it's the asynchrony. Ok that makes sense! Finally!	1262347151981543428
18-05-20 11:39	**Nadim Kobeissi**	But for Signal it wouldn't work because sessions are essentially established when you first message someone and last until one of you changes phones	1262347196210561029
18-05-20 11:40	**Nadim Kobeissi**	This protocol guarantees post-compromise security on a session-by-session basis which is 100% appropriate	1262347291140206603
18-05-20 11:41	**Nadim Kobeissi**	What you could say is the following: "This protocol was modeled and prototyped using Verifpal, and then confirmed to obtain confidentiality, authentication and per-session post-compromise security via protocol analysis under Verifpal's formal analysis framework"	1262347689594888196
18-05-20 11:42	**Nadim Kobeissi**	To be honest it would be totally a huge deal for us if we could say you used Verifpal for this, I won't lie, that would really be incredible	1262347782804975622
18-05-20 11:42	**Nadim Kobeissi**	And I'd be very happy to work on Verifpal to cater to your use cases and to implement feedback	1262347833228787717
18-05-20 11:54	**Nadim Kobeissi**	btw did you know that you can use Verifpal to automatically translate your model to a Coq model or ProVerif model?	1262350749469741066
18-05-20 11:54	**Nadim Kobeissi**	Also soon to a Go implementation	1262350772043485189

18-05-20 12:54	**Nadim Kobeissi**	Please let me know if you think we could say something publicly regarding this!	1262365993634054149
18-05-20 14:18	**Max Krohn**	Sure thing, Will do, but nothing yet though, we are still in the draft phases and have to pass a bunch of reviews.	1262387024545427462
18-05-20 14:48	**Nadim Kobeissi**	Got it	1262394632933122052
18-05-20 14:53	**Max Krohn**	Personally, I had an extremely positive interaction with the software and it makes 10x more confident about this protocol. You know where I am on this :)	1262395847435829253
18-05-20 14:54	**Max Krohn**	You are going to be Yvgeniy Dodis out of a job!	1262396138797305860
18-05-20 14:54	**Max Krohn**	be -> put	1262396158741295110
18-05-20 15:09	**Max Krohn**	What's the best critique so far of Verifpal?	1262399982696566793
18-05-20 15:16	**Nadim Kobeissi**	We've already answered it	1262401687265951748
18-05-20 15:16	**Nadim Kobeissi**	(Very recently)	1262401708371652613
18-05-20 15:16	**Nadim Kobeissi**	It was the USENIX review of our USENIX submission	1262401764285992964
18-05-20 15:16	**Nadim Kobeissi**	We answered it with our CCS submission which we made last week	1262401797022498821
18-05-20 15:16	**Nadim Kobeissi**	Give me your email	1262401804777684999
18-05-20 15:17	**Nadim Kobeissi**	I'll send you our CCS submission which includes the USENIX review and our rebuttal	1262401845978333190
18-05-20 15:17	**Max Krohn**	max@keyba.se	1262402051989999633
18-05-20 15:18	**Max Krohn**	thanks!	1262402102904737797
18-05-20 15:18	**Nadim Kobeissi**	Please keep this confidential btw it's our CCS submission	1262402185536647174
18-05-20 15:18	**Max Krohn**	of course, will do	1262402219493806084
18-05-20 15:19	**Nadim Kobeissi**	Sent	1262402478655639561
18-05-20 15:19	**Nadim Kobeissi**	See "Review A" in the Appendix	1262402506329595909
18-05-20 17:10	**Max Krohn**	what a load	1262430299608227849
18-05-20 17:10	**Max Krohn**	reminds me of why i don't mind being on the "outside"	1262430349566644229
18-05-20 17:10	**Max Krohn**	there is basically nothing of substance here	1262430433440137220
18-05-20 17:10	**Max Krohn**	in this review	1262430448560615431
18-05-20 17:11	**Nadim Kobeissi**	Yupppppppppp	1262430589388554247
19-05-20 21:30	**Max Krohn**	we think we found a protocol that verifies that shouldn't	1262858219409616900
19-05-20 21:36	**Max Krohn**	OK, this is our original protocol	1262859742332039174
19-05-20 21:36	**Max Krohn**	https://t.co/jHXsUMe80B	1262859749370089481
19-05-20 21:37	**Max Krohn**	This is one verifies (but I don't think it should)	1262859892903247876
19-05-20 21:37	**Max Krohn**	https://t.co/dJRr4nvcSy	1262859897307312139
19-05-20 21:37	**Max Krohn**	This one doesn't verify:	1262859944325455878
19-05-20 21:37	**Max Krohn**	https://t.co/LYYtKm5Yvl	1262859996305526789

19-05-20 21:38	**Max Krohn**	(hopefully they are off by a few small edits gb v [gb], etc)	1262860313071882245
19-05-20 21:39	**Max Krohn**	I don't see how v2 and v3 would yield different results	1262860369011396612
19-05-20 23:47	**Max Krohn**	Upon further reflection, maybe there is a good explanation for it, that either Bob or Charlie aborts, preventing the secret from being learned. But I don't fully understand.	1262892567332564996
20-05-20 4:13	**Nadim Kobeissi**	Looking into it now	1262959648644227082
20-05-20 4:13	**Nadim Kobeissi**	btw you should join our Discord	1262959663454269444
20-05-20 4:17	**Max Krohn**	yeah i should	1262960517209096198
20-05-20 4:17	**Max Krohn**	i should also go to bed!	1262960531205500938
20-05-20 4:17	**Max Krohn**	you wake up very early it seems	1262960563895840773
20-05-20 4:17	**Nadim Kobeissi**	Give me a minute I might be able to figure out your thing	1262960604769390596
20-05-20 4:22	**Max Krohn**	i don't really care about my thing, but i was just worried that verifpal didn't say it was buggy	1262961939170365445
20-05-20 4:22	**Nadim Kobeissi**	Uh	1262961975966998534
20-05-20 4:22	**Nadim Kobeissi**	z2 doesn't verify here	1262961989371998212
20-05-20 4:23	**Max Krohn**	that would be the issue, lemme triple-check	1262962082124791812
20-05-20 4:23	**Nadim Kobeissi**	https://t.co/9qzPs8QFlI	1262962087736868869
20-05-20 4:23	**Nadim Kobeissi**	Make sure you're using the latest Verifpal version (0.13.5)	1262962145463074821
20-05-20 4:23	**Max Krohn**	oh!	1262962162240237572
20-05-20 4:23	**Max Krohn**	i am not!	1262962168410050564
20-05-20 4:23	**Nadim Kobeissi**	It contains a few important fixes	1262962170737889290
20-05-20 4:23	**Max Krohn**	did you just fix a big	1262962181970239492
20-05-20 4:23	**Max Krohn**	bug	1262962193554976776
20-05-20 4:23	**Max Krohn**	oh!	1262962196742635529
20-05-20 4:23	**Max Krohn**	ok thx	1262962201637400588
20-05-20 4:23	**Max Krohn**	sorry to bother you	1262962212123160582
20-05-20 4:24	**Nadim Kobeissi**	Dude are you kidding? You're the best thing that's happened all month	1262962264660983817
20-05-20 4:24	**Nadim Kobeissi**	I'm incredibly happy to hear you're liking Verifpal and honored that it might help a thing as impactful as Zoom	1262962337629253636
20-05-20 4:24	**Nadim Kobeissi**	Please definitely bug me all the time	1262962376518914063
20-05-20 4:26	**Nadim Kobeissi**	I'm running z2 on the older Verifpal version (0.13.4) to see if it was indeed the latest hotfix release that changed the result	1262962891445145604
20-05-20 4:26	**Nadim Kobeissi**	Yes it was!	1262962968981049348
20-05-20 4:27	**Nadim Kobeissi**	Indeed the older version says z2 passes	1262963007900078087
20-05-20 4:27	**Nadim Kobeissi**	Yup this was fixed recently	1262963031018999819

20-05-20 4:27	**Nadim Kobeissi**	Here's the commit	1262963041492258822
20-05-20 4:27	**Nadim Kobeissi**	https://t.co/YLKFdvBf3a	1262963117174280197
20-05-20 4:34	**Max Krohn**	Ah, thanks for the pointer, seems like it was just fixed. We are past the original protocol which we are now happy about and are arguing about a protocol as in redphone circa 2013 when you exchange words in a meeting to detect MITM. it's interesting how hard the intuitions are here. i suspect our cryptographer is wrong here but i haven't proven it one way or the other. might be a job for tomorrow, it is late!	1262964947752976389
20-05-20 4:36	**Max Krohn**	i feel like i am back in grad school with paper deadline and the feeling that the paper is totally broken for a different reason every hour.	1262965290293497860
20-05-20 13:32	**Max Krohn**	Hi Nadim, ok next question. This protocol fails for a reason I disagree with. The context here is that we have a protocol for showing "security codes" in the app and then having the reader read them out.	1263100168917979140
20-05-20 13:32	**Max Krohn**	https://t.co/A6wmyVP6dD	1263100175750443013
20-05-20 13:43	**Nadim Kobeissi**	Looking	1263103011213082629
20-05-20 14:18	**Nadim Kobeissi**	I don't see the problem	1263111964781395972
20-05-20 14:19	**Nadim Kobeissi**	geb is unguarded, attacker replaces it with evil public key, I encrypt the session key to evil public key	1263112152367366148
20-05-20 14:19	**Nadim Kobeissi**	Of course the attacker will get sesskey	1263112198030856196
20-05-20 14:21	**Nadim Kobeissi**	https://t.co/DOUkcK1w9E	1263112607747264517
20-05-20 14:21	**Nadim Kobeissi**	What results were you expecting?	1263112628383211524
20-05-20 14:22	**Nadim Kobeissi**	https://t.co/TI2VQKKasR	1263112748671602693
20-05-20 14:33	**Max Krohn**	Well the output say it can mangle gae which is why I was confused	1263115714786885637
20-05-20 14:34	**Nadim Kobeissi**	Yes that part is wrong	1263115846488068100
20-05-20 14:34	**Nadim Kobeissi**	It should say geb	1263115859356246021
20-05-20 14:34	**Nadim Kobeissi**	But the fact that the query is contradicted is not wrong	1263115912548421639
20-05-20 14:34	**Nadim Kobeissi**	I'm looking into that weird output now	1263115930239995911
20-05-20 14:34	**Max Krohn**	ok, well here is the larger picture	1263115977711026180
20-05-20 14:35	**Max Krohn**	i started with a protocol that i thought to be equivalnet, which passes, and then i tried to refine it, and it didn't pass	1263116044220223493
20-05-20 14:35	**Max Krohn**	let me also send you the protocol that passes	1263116100407099396
20-05-20 14:36	**Max Krohn**	https://t.co/oLWmZK1XiZ	1263116371518504967
20-05-20 14:37	**Max Krohn**	And at a high level, geb isn't actually unguarded, since it's part of ga_enc, which is guarded	1263116624162435078

20-05-20 14:42	**Max Krohn**	... in practice i don't see a difference between v5 and v6, it's seems like reordering of computations that aren't dependent on each other....	1263117827801788422
20-05-20 14:42	**Max Krohn**	of couse i could be totally wrong	1263117875163942916
20-05-20 14:48	**Nadim Kobeissi**	https://t.co/ulWvj8XcqV	1263119487936724996
20-05-20 14:51	**Nadim Kobeissi**	It's because you're forcing the check on the decryption of ga_enc in z6	1263120220832632841
20-05-20 14:52	**Nadim Kobeissi**	That check will never succeed if there's a MITM	1263120312008429574
20-05-20 14:52	**Nadim Kobeissi**	These results are correct	1263120430010957829
20-05-20 14:52	**Nadim Kobeissi**	Z5 should fail and Z6 should pass	1263120460809633796
20-05-20 14:53	**Nadim Kobeissi**	In Z6 you're doing the voice-over auth of ga before even generating sesskey	1263120783183839236
20-05-20 14:54	**Nadim Kobeissi**	That's what's making the difference	1263120797494804484
20-05-20 14:55	**Nadim Kobeissi**	Just pushed 0.13.6 which fixes the incorrect output regarding the confidentiality trace in Z5, please update (will take 5 minutes to hit Homebrew)	1263121144913244165
20-05-20 14:55	**Max Krohn**	thanks nadim, we will iterate and get back to you!	1263121284579409924
20-05-20 15:32	**Max Krohn**	is the scuttlebutt.vp protocol supposed to verify?	1263130499997929478
20-05-20 15:33	**Max Krohn**	ok, no, in the docs...	1263130776180264965
20-05-20 15:34	**Max Krohn**	actually i don't know	1263131036701143046
20-05-20 15:37	**Nadim Kobeissi**	I don't remember what the result is supposed to be for that one it's been months	1263131754233290757
20-05-20 15:37	**Nadim Kobeissi**	But it was checked for correctness	1263131815155568645
20-05-20 15:46	**Max Krohn**	it fails on 0.13.6, i was just curious, that might be a regression if it's supposed to work	1263134079203057668
20-05-20 15:52	**Max Krohn**	Well, I feel bad for taking up so much of your time. But I would say, we have one more question we can't figure out on our own. My colleague who is an actual cryptographer is also trying to model this voice-over protocol, but from a different direction. He came up with this stripped-down protocol, and we can't reason successfully about why it's failing. It should see that the assertion should stop the protocol from succeeding, and there are no long-term keys, so a failed protocol should be useful in the future. Again, thanks for all your help, sorry for taking up so much of your time!	1263135496680738820
20-05-20 15:52	**Max Krohn**	https://t.co/MLCE40r7YK	1263135500694683656
20-05-20 15:53	**Max Krohn**	(should be useful in the future -> should not be useful in the future)	1263135649365921797

20-05-20 15:55	**Nadim Kobeissi**	Wait what?	1263136150 249705484
20-05-20 15:55	**Nadim Kobeissi**	Yeah if Scuttlebutt fails that's not a problem	1263136260 157313028
20-05-20 15:59	**Nadim Kobeissi**	Hold on I'm in the metro, will look at this when I get home	1263137175 903879175
20-05-20 16:00	**Nadim Kobeissi**	Can you paste me the query output for ant2	1263137551 470284804
20-05-20 16:00	**Max Krohn**	sure thing	1263137573 020598276
20-05-20 16:01	**Max Krohn**	https://t.co/K8kQp8pFRd	1263137702 951739400
20-05-20 16:01	**Max Krohn**	oy let me pick a better terminal	1263137754 751393798
20-05-20 16:02	**Max Krohn**	https://t.co/7uLclTG3JR	1263137925 476352005
20-05-20 16:08	**Nadim Kobeissi**	Attacker can't modify the guarded sesskeys sure	1263139578 812289030
20-05-20 16:08	**Nadim Kobeissi**	But	1263139584 227057669
20-05-20 16:09	**Nadim Kobeissi**	It can still force them to agree on bad sesskeys by mitming geb from the get go	1263139891 732512772
20-05-20 16:10	**Max Krohn**	how will that pass the ASSERT()?	1263140086 025261062
20-05-20 16:10	**Max Krohn**	won't alice and bob abort?	1263140130 405171205
20-05-20 16:10	**Nadim Kobeissi**	This output is correct	1263140138 697273351
20-05-20 16:11	**Nadim Kobeissi**	One sec	1263140292 380766212
20-05-20 16:11	**Nadim Kobeissi**	Sorry terrible metro reception	1263140329 429045254
20-05-20 16:11	**Max Krohn**	no worries	1263140365 613359112
20-05-20 16:11	**Max Krohn**	thx so much for your help	1263140381 165830149
20-05-20 16:12	**Nadim Kobeissi**	Oh wow interesting	1263140481 678147594
20-05-20 16:12	**Nadim Kobeissi**	I see the issue now	1263140513 093468165
20-05-20 16:12	**Nadim Kobeissi**	I'm still not convinced this is a false result 😁😁😁	1263140586 275647492
20-05-20 16:12	**Nadim Kobeissi**	Investigating	1263140607 188492296
20-05-20 16:14	**Nadim Kobeissi**	Can you try something	1263141044 742426634
20-05-20 16:14	**Nadim Kobeissi**	Set attacker to passive and leak eb at the start of the session	1263141085 599215622
20-05-20 16:14	**Max Krohn**	yes one sec	1263141136 211853319
20-05-20 16:15	**Nadim Kobeissi**	Let me know what the result is	1263141340 545777668
20-05-20 16:15	**Max Krohn**	same result i think	1263141355 678818309
20-05-20 16:15	**Nadim Kobeissi**	OK	1263141388 507648007
20-05-20 16:16	**Max Krohn**	i'll do a screen cap just to be sure	1263141443 490721797
20-05-20 16:17	**Max Krohn**	https://t.co/7hkzLCoMgo	1263141745 572958212
20-05-20 16:17	**Nadim Kobeissi**	Yup this is a legit result:D	1263141849 407066119
20-05-20 16:18	**Nadim Kobeissi**	Looks like Verifpal found an attack you fellas would have missed otherwise 😎😎😎	1263141991 749165061
20-05-20 16:18	**Nadim Kobeissi**	Will explain when I get home	1263142018 018050057
20-05-20 16:18	**Nadim Kobeissi**	Give me 30 min	1263142034 405294098
20-05-20 16:28	**Max Krohn**	oh super, i am so excited to hear it!	1263144525 612154886

20-05-20 16:33	**Max Krohn**	if you'd like to meet via videoconf that can be done too	1263145886642778116
20-05-20 16:38	**Nadim Kobeissi**	How can I call you	1263147004554883076
20-05-20 16:38	**Nadim Kobeissi**	I have WhatsApp Signal	1263147032447004681
20-05-20 16:40	**Max Krohn**	either is fine, but do you want to do a screenshare?	1263147505509941252
20-05-20 16:40	**Nadim Kobeissi**	I'm walking my dog	1263147561818480646
20-05-20 16:40	**Max Krohn**	hahah then no	1263147593347084292
20-05-20 16:40	**Nadim Kobeissi**	15 more mins	1263147623965429764
20-05-20 16:40	**Max Krohn**	ok i am at 1-917-215-8091 when you get a chance	1263147649382993927
20-05-20 16:40	**Max Krohn**	lemme make sure i have signal installed	1263147664457240581
20-05-20 16:41	**Max Krohn**	sorry, i have to wipe all of my keys and destroy all my trust relationships because i got a new phone	1263147905126449163
20-05-20 16:42	**Max Krohn**	signal: trust on everytime someone gets a new phone!	1263148082616827916
20-05-20 17:15	**Max Krohn**	Hey I need to disappear into meetings soon.	1263156292908179461
20-05-20 17:19	**Nadim Kobeissi**	Okay I'm ready	1263157459977453573
20-05-20 17:19	**Nadim Kobeissi**	Still around?	1263157501194797061
20-05-20 17:20	**Max Krohn**	yes	1263157638273077252
20-05-20 17:41	**Max Krohn**	thanks so much, both ant2.vp and z5.vp suffered from the same philosophical failure now that i see it	1263162845304434693
20-05-20 17:44	**Nadim Kobeissi**	:D	1263163699294060548
20-05-20 17:44	**Nadim Kobeissi**	I think Zoom should let us write a blog post about how Verifpal helped you guys design your new protocols :D :D :D	1263163812435369990
20-05-20 17:45	**Nadim Kobeissi**	https://t.co/2zEquxee4G	1263163884879388676
21-05-20 1:28	**Max Krohn**	So here's something else that I think is a limitation of verifpal, but I've been know to be wrong. Look at the two following protocols, they are different only in the order in which alice and bob act, but there is no reason why one needs to act before the other, as there is no communication between them. But yet one protocol verifies and the other does. My hunch is that verifpal is running the script in the order it's specified and not reordering actions sufficiently. Just a guess. Two files to follow....	1263280353525075973
21-05-20 1:28	**Max Krohn**	verifies: https://t.co/oLWmZK1XiZ	1263280378548310020
21-05-20 1:28	**Max Krohn**	fails: https://t.co/enN9FrGeLQ	1263280449318793222
21-05-20 6:23	**Nadim Kobeissi**	Will look into it in a bit :-) this is really fun!	1263354776823218186
21-05-20 6:42	**Nadim Kobeissi**	Yeah man this is obviously going to fail	1263359407368409092
21-05-20 6:42	**Nadim Kobeissi**	Same reason as yesterday	1263359429468176388

21-05-20 6:42	**Nadim Kobeissi**	In z7 Alice sends sesskey before strong authentication between Alice and Bob can be established	1263359523387060228
21-05-20 10:16	**Max Krohn**	But why does one work and the other fail? They should either both work or both fail.	1263413325079207940
21-05-20 10:17	**Max Krohn**	(I agree they should both fail)	1263413557309382661
21-05-20 10:34	**Max Krohn**	In other words, the verifier should have reordered z6 automatically to be like z7, but it didn't.	1263417936804544516
21-05-20 10:41	**Nadim Kobeissi**	Let me investigate and get back to you	1263419698424819727
21-05-20 11:57	**Nadim Kobeissi**	You know, it's true that this behavior is certainly non-obvious	1263438794306523140
21-05-20 12:01	**Nadim Kobeissi**	In Z6, Bob is aborting the protocol before sesskey can be encrypted under false keys, in Z7 that is not the case	1263439723927875588
21-05-20 12:01	**Nadim Kobeissi**	So in Z7 the protocol abort/parallel execution scenario works	1263439784615317509
21-05-20 12:01	**Nadim Kobeissi**	That is why you have this result	1263439876105609222
21-05-20 12:02	**Nadim Kobeissi**	But I do agree that this is not at all communicated clearly, not even close	1263439914789675024
21-05-20 15:08	**Max Krohn**	It might be a deeper architectural question, or my failure to understand, but why does the model run Alice and Bob in serial, it should have the freedom to reorder them if their computations do not depend on communications with each other. I mean, this is what a bad guy would do. He would slow down Alice and speed up Bob, or vice versa. In this particular example, how is Bob's aborting the protocol actually affecting Alice's generation of sesskey? It's almost as if there's trusted channel between them communicating this, but that feels like a shortcoming in the model checker that makes attackers artificially weak, since there's no reason to assume that trusted channel exists.	1263486746941165572
23-05-20 7:34	**Nadim Kobeissi**	Hey!	1264097280652697604
23-05-20 7:34	**Nadim Kobeissi**	https://t.co/EaqEg1s7Q0	1264097317470326790
23-05-20 7:34	**Nadim Kobeissi**	Just saw this, congrats!!	1264097336562761732
23-05-20 7:34	**Nadim Kobeissi**	I'm surprised to see that Verifpal wasn't mentioned or that the Verifpal paper wasn't cited, any particular reason?	1264097435913195524
23-05-20 7:38	**Nadim Kobeissi**	To be honest I think it's pretty shocking that there would be no citation or mention after all the time we spent discussing the protocol and Verifpal	1264098390675271684