Exhibit B

- From | Isis
- Sent | Fri, 09 Oct 2015 17:48:28 UTC
- Erase | Fri, 16 Oct 2015 18:06:33 UTC
- Retain | true

> So, looks like I'm going to China from the 1st or 5th or so. Will be visiting Bitcoin mining operations mainly.
>

Neat. Cover yourself in cameras. Both for the amazing sights and to better notice the agents tailing you on rotation. Also, don't let any electronics you care about out of your sight, for seriously. As in: sleep with your laptop under your pillow. Also, I didn't carry my OpenPGP key or SSH keys when I went there (I normally don't carry the master certification key, but in this case I carried none of my key).

> You've told me about your "interesting" experiences in China... what should I know? In particular, do you think they're crazy enough that I'd be survailled based on knowing you? Based on my position within Bitcoin? I'm probably the 2nd or 3rd best known Bitcoin dev out there. :/

Based on knowing me… meh… not so likely. But based on working on Bitcoin and publicly expressing interest in having better censorship circumvention built into Bitcoin, and the fact that you've attended a few Tor developer meetings… yeah, they will likely watch you closely. It's not uncommon to be followed by multiple people, have your hotel room searched without notice, and have people/agents try to record anything you attempt to say in private to another person. Be super careful. Also, Hong Kong is a different animal, and they mostly despise the government of the mainland, but they're careful not to state those opinions too strongly. HK still does have secret police, and also undercover agents from the mainland who will both want info from you. In my case, I was also followed by some fat, white, spooky American dude (probably CIA) whose cover was pretending to read Chinese newspapers (they were usually upsidedown).

```
  - From   | Isis
  - Sent   | Tue, 20 Oct 2015 17:57:27 UTC
  - Erase  | Tue, 27 Oct 2015 20:28:35 UTC
  - Retain | true

> How was your talk?
>

It went well.  The audience wasn't exactly as math/crypto inclined as I'd have
hoped, but at least they mostly all knew what tor was and used it everyday.
```

```
  - From   | Isis
  - Sent   | Tue, 27 Oct 2015 22:53:13 UTC
  - Erase  | Wed, 04 Nov 2015 04:06:10 UTC
  - Retain | true

> FYI I'm going to be in SF on Nov 1st for a few days.
>

hey hey, i'm living in germany until 25 nov, then not sure where after that, but
probably not SF because it's too expensive and i've no reason to be there.
```

- From | Isis
- Sent | Mon, 02 Nov 2015 21:23:36 UTC
- Erase | Mon, 09 Nov 2015 21:46:09 UTC
- Retain | true

> > > > hey hey, i'm living in germany until 25 nov, then not sure where after that, but
> > > > probably not SF because it's too expensive and i've no reason to be there.
> > >
> > > Ah cool! Berlin is nicer than SF. (but I don't surf and like cold weather...)
> > >
> > > Maybe move to Amsterdam next? :) How's things going?
> > >
> >
> > Yes, I'm quite strongly considering that I should live in NL. I've been here at
> > Technisches Universität Eindhoven all week, and have made friends with the whole
> > cryptography department. :) It's amazing. I really forgot what it was like to
> > be around people who are free to be curious for curiosity's sake.
>
> Go for it! Are you officially doing anything with them yet? I remember you said
> you might manage to get a PhD or something.

I'm going to work with one of their postdocs soon to try using their pairing-based crypto library for the thing I'm working on. We'll see where that goes…

> Did the Tor bridge thing with OTF finally go through?

Uh. Heh. A week ago, they said, "Yeah, I'm talking with compliance right now about getting your contract together, and the start date is 23 Oct, so you can start working." And I responded, "Great, thanks!" and then decided fuck working on a contract I haven't signed because I've learned that lesson the hard way several times.

How's your Chaincode(? goddamnit I can never remember the names of bitcoin startups) job prospectives coming along?

- From | Isis
- Sent | Wed, 04 Nov 2015 13:02:32 UTC
- Erase | Wed, 11 Nov 2015 18:09:12 UTC
- Retain | true

> BTW how did you wind up signing Matt Corallo's key? He said he gave his
> business card to Mike, but not you...

Mike loses things and doesn't sign keys, so I stole the card from Mike just after Matt handed it to him, while we were all sitting at the table together at Graçias Madré. It seemed useful to sign it so that I'd have some form of direct authentication for Matt later. Plus, if Mike ever wants to authenticate Matt, he'll probably ask me to verify the damned thing anyway since yeah… he has this stupid thing against signing keys (even locally!). ¯_(ツ)_/¯

- From | Isis
- Sent | Wed, 04 Nov 2015 13:19:50 UTC
- Erase | Wed, 11 Nov 2015 18:10:57 UTC
- Retain | true

> > > Go for it! Are you officially doing anything with them yet? I remember you said
> > > you might manage to get a PhD or something.
> >
> > I'm going to work with one of their postdocs soon to try using their
> > pairing-based crypto library for the thing I'm working on. We'll see where that
> > goes…
>
> The Tor bridge anonymous credential thing right? Nice!

Yep.

> How's funding working on that? I guess the postdoc must be funded by the
> university right?

It goes. The funding is the contract thing that I mentioned previously. And,
yep, the postdoc has their own funding to make the library, and is already
mostly finished, so this would be like the icing on the deathcake to have
someone from Tor use their library for a project, since that makes the paper
shinier. Also, they want someone who's used a lot of crypto libraries to test
out the APIs and stuff and complain when the library is a bitch to use.

> > > Did the Tor bridge thing with OTF finally go through?
> >
> > Uh. Heh. A week ago, they said, "Yeah, I'm talking with compliance right now
> > about getting your contract together, and the start date is 23 Oct, so you can
> > start working." And I responded, "Great, thanks!" and then decided fuck working
> > on a contract I haven't signed because I've learned that lesson the hard way
> > several times.
>
> Oh yeah? How've you been screwed over before by this?

One, there's the chance that they don't hand me the contract, or it has some
stipulations again that would cause me to not sign it. Then there's the problem
of timing things correctly, like if they backdate my contract to Oct 22 like
they are doing, then it ends next Oct 22 and I have to time finishing it right
and getting more funding after in ways that quickly add more bureaucracy and are
more annoying. Also, there is the problem that the funder "needs" status
reports of my work on a certain day of the month for me to get paid, and I get
paid once per month, and I shouldn't send reports if I'm not getting paid, so
because of the backdating issue, if the total actual period of the contract is,
say, 10 months, then there are two months where it is unclear what reporting
obligations I have and how the fuck I am supposed to bill, or if I am supposed
to back-/forward- date status reports or what. Mostly it's just painful. Also,
it makes asking for contract extensions painful and costly (like I'd get less
money overall).

> > How's your Chaincode(? goddamnit I can never remember the names of bitcoin
> > startups) job prospectives coming along?
>
> Surprisingly you got the name right! :)

lifewinning++

> Chaincode last said they still have an
> offer on the table, but it looks like I'll be signing a contract with R3 very
> shortly.

Who's R3?

> The good thing is it has a Reserved IP thing where part of what I'm
> working on for them will be 100% open source - they get a non-exclusive license

> to do what they want with the IP, I get the ability to release under an open
> source license of my choosing. (which should extingish any patents as well)

How does that cause patents to go away?

> OTOH it's a full time contract, so I'll be quitting other consulting work - it
> also makes me look like an employee which is really not optimal...

Not optimal in terms of travelling to/spending the majority of your time in the US? Wouldn't this make it easier for you to get an H1(? I think that's the number) visa?

> I probably
> spent like $2k last in the past two weeks on my lawyer negotiating it, which
> was a fucking exasperating process. But at $14k/month the pain is probably
> worth it, and it'll help get that fintech in the public sphere whether they
> want to or not.

Everytime you say "fintech" my brain thinks:
https://www.youtube.com/watch?v=d3u86DPd7qc&list=PLVBPIVPWaZrs53OdNXOH1_4TYwd84_GYY

> It's also my proofchains work, which is stuff I've been wanting
> to do for ages now, and I think it can be reused to make Bitcoin-type systems
> actually scale for once.

Yay! I'm glad you finally get to work on this. :)

> The totally crazy thing is that Mike Hearn got hired by them too and I'll be
> working with him.

O_o

Let's play spot the fed! Oh look. There's Mike Hearn. That was easy.

Just don't let Hearn stray you to the dark side. Or shit-for-brains side or saboteur side or whatever his game is. :)

```
  - From   | Isis
  - Sent   | Thu, 14 Jan 2016 14:16:56 UTC
  - Erase  | Thu, 21 Jan 2016 22:31:53 UTC
  - Retain | true

> I was reading through Rivest's sexp thing, http://people.csail.mit.edu/rivest/Sexp.txt
>
> I've got some crazy scheme where a merkelized s-expression makes a lot of
> sense; you ever come across such a thing? It's interesting that Rivest's work
> suggests simply hashing the whole, canonically serialized, sexp.
>
> ...and yes, I'm making a merkelized lisp, kinda.

Sort of, but sort of not really.  The closest I know of is this hashring trie
structure hybrid thing which uses sexps to make insertion and lookup faster, but
I totally made it up for my specific use case because no such thing existed and
also it's not done/fully-tested/merged yet:

https://gitweb.torproject.org/user/isis/bridgedb.git/tree/bridgedb/tries.py?h=fix/12505-
11330-hashrings_r1

or

https://github.com/isislovecruft/bridgedb/blob/fix/12505-11330-
hashrings_r1/bridgedb/tries.py

but also the trie part is not necessarily balanced, so it's not merklisable
afaik.
```

```
  - From   | Isis
  - Sent   | Thu, 24 Mar 2016 15:11:13 UTC
  - Erase  | Thu, 31 Mar 2016 23:04:00 UTC
  - Retain | true

> Heh, finally got around to getting pond installed on my new Qubes install on my
> laptop... er, I mean, finally copied the statically compiled gopkg...
>
> > > Paige told me she thought you were "rad" :)
> > >
> > > I wish I could have come out!
> > >
> >
> > Heh, it was quite a bad week for me, but I was glad to meet Paige as well. :)
>
> Aww. :(
>
> Where are you these days? I might make it to Paris in early May for a fintech
> conference.
>

Theoretically, I live in Berlin.  But I travel constantly.  Literally, I am in
Berlin for like 3 days per month.

> Also, I think you'd like the paragraph I managed to put into a Totally
> Official, NDAed and all, report I wrote for the Australia Post:
>
>     Even in less dramatic scenarios there is an inherent conflict between making
>     the biometrics system easy to use, while making it difficult for identity
>     thieves to surreptitiously steal that identity by scanning your body. We can
>     illustrate this conflict very clearly by considering a highly effective, yet
>     rather unplatable biometric secret key: simply tattoo your secret key onto your
>     genitals. I don't think we need to explain why this scheme would be very
>     difficult for thieves to compromise, and it does have the advantage that most
>     users will naturally take the right precautions to prevent such theft. But
>     let's be frank, the idea is ridiculous. Biometric secret keys aren't much
>     better.
>

ROFL that is amazing. :)
```

```
  - From   | Isis
  - Sent   | Mon, 25 Apr 2016 17:37:01 UTC
  - Erase  | Mon, 02 May 2016 23:33:43 UTC
  - Retain | true

> I'm writing an article on some leaked docs I got from a MIT scheme to add AML to
Bitcoin.
>
> Mind taking a look at this paper?

I have negative free time to do that right now. :/

> I'm trying to figure out what anonymity
> properties this anonymity EPID scheme actually has. Seems that it's critical
> that the permission issuer, IdP-PI, and permissions verifiers, IdP-PV's, don't
> collude, but I'm not 100% sure I understand why. The paper in section E.
> Discussion says that the user remains anonymous to the IdP-PV, but I assume
> what they really mean is that the user remains *pseudo-anonymous*, meaning each
> pubkey the user enrolls can be linked together by the IdP-PV. If that is true,
> then it's true that the IdP-PI and IdP-PV can collude to deanonymise the user.
>
> Does that sound correct to you?

That is generally how IdP systems work, yes.  This is usually done so that user
blacklisting/whitelisting can still occur without using more modern crypto.

> Also, I have a new OTR fingerprint: 41b3 58a2 e336 a530 b736 d783 28c6 150d b320 e959

Cool, thanks!
```

- From | Isis
- Sent | Sun, 01 May 2016 00:43:53 UTC
- Erase | Sun, 08 May 2016 02:36:14 UTC
- Retain | true

> Looking like I may be in Zurich May 19th to 23rd, then Amsterdam to the 27th or
> so, then Arnhem, then back to Amsterdam to fly home on June 1st or so. You
> going to be around? Also, I could probably make use of a couch for some of that
> time if you have any suggestions

It's a bit of an urgent situation. Can you please embed a hash of my most recent blog post in the blockchain?

```
  - From   | Isis
  - Sent   | Wed, 25 May 2016 09:40:03 UTC
  - Erase  | Wed, 01 Jun 2016 11:37:26 UTC
  - Retain | true

I presume you've seen that this year's Underhanded Crypto Contest is to backdoor
a cryptocurrency? :)

https://underhandedcrypto.com/2016/01/27/rules-for-the-2016-underhanded-crypto-contest/
```

- From | Isis
- Sent | Wed, 25 May 2016 12:15:02 UTC
- Erase | Wed, 01 Jun 2016 12:30:16 UTC
- Retain | true

> > I presume you've seen that this year's Underhanded Crypto Contest is to backdoor
> > a cryptocurrency? :)
> >
> > https://underhandedcrypto.com/2016/01/27/rules-for-the-2016-underhanded-crypto-contest/
>
> YES!!!! Oh man, I gotta come up with something for this... I'm thinking I might
> backdoor a merkle tree algorithm actually, as I know of a few subtle algo-level
> exploits that many miss...
>
> BTW I didn't hear back from you about your talk tomorrow, so I'm going to the
> security in times of survaillance thing at Eindhoven uni tomorrow, and the
> crypto working group thing in utrecht the day after.

i wasn't planning on going.

over the past five months, three people (one of my tor coworkers, a journalist, and someone who works for a medium-sized organisation closely connected to tor) have come forward to me with horrible stories of jake applebaum raping them, then jake threatened me on multiple levels to try to convince me not to report it. my Ph.D. advisors banned him from coming to several conferences, and tried to tell tanja (jake's advisor) but she would not listen. tomorrow, as i understand it, there will be some disruption to his talk. if i have to face him in person, i would prefer to have my rifle. feel free to make a statement by very loudly standing up at the beginning of his talk and walking out, lol. others should be doing the same. also feel free to spread the word, because the shit is about to go down in tor and he'll be fired, and academia should reject him as well.

i'm not going because this issue, combined with the FBI bullshit, has been giving me panic attacks and my professors and my partner think i should not attend.

my partner will be there. he's also canadian, adorable, and genius; his name is harry and he has pink and blue hairs.

idk maybe i will go, but i'm sitting in berlin right now on no sleep so yeah.