






Exhibit I





 Home


 Explore


 Notifications

 Messages


 Bookmarks


 Lists


 Profile


 More


Tweet

 Messages


 Bookmarks


 Lists


 Profile


 More


Tweet

 Messages

 Bookmarks


 Lists

 Profile

 More

Tweet

Thread

 **Peter Todd** @peterktodd · Feb 5
(fixed) Zcash counterfeiting vulnerability: z.cash/blog/zcash-counterfeiting-vulnerability


"This vulnerability is so subtle that it evaded years of analysis by expert cryptographers focused on zero-knowledge proving systems"

Reality is bleeding edge crypto is risky; second inflation bug they've had.

ELECTRIC COIN CO


Zcash Counterfeiting Vulnerability Successfully Remediated - Electric Coin...
Eleven months ago we discovered a counterfeiting vulnerability in the cryptography underlying some kinds of zero-knowledge proofs. This post...
electriccoin.co

16 132 340

 **Peter Todd** @peterktodd · Feb 5
(first being caught prior to release)


BTC has categorically worse privacy than ZEC on L1, but the trade-off is a safer system re: total loss. Had this been exploited, it could have easily been a hundreds of millions of dollars loss.

2 2 49

 **Peter Todd** @peterktodd · Feb 5

On BTC an inflation bug is very likely to get caught quickly, even if exploited, because of the transparency. That might be a few days shutdown at worse: awful, but survivable even in the worst case.


4 7 48

 **Peter Todd** @peterktodd · Feb 5

On a personal note, this part is interesting. Based my interactions with them, sounds like they deleted it publicly, then managed to actually lose it for real. WTF


To exploit the counterfeiting vulnerability, an attacker would have needed to possess information found in the large MPC protocol transcript that was made available shortly after the launch of Zcash. This transcript had not been widely downloaded and was removed from public availability immediately upon discovery of the vulnerability to make it more

3 5 29

 **Peter Todd** @peterktodd · Feb 5

Remember my interactions with Zooko: twitter.com/peterktodd/status/9811111111

That's after the bug is fixed, so no need to make up a story; if they were being honest they'd admit they screwed up and actually lost it, which the blog post glosses over.

 **Peter Todd** @peterktodd · Nov 14, 2018

@zooko I'm going to reply here because this isn't a security issue in the normal sense. We're not fixing a vulnerability here, we're fixing an embarrassing lack of record keeping that only shows potential incompetence or fraud.

[Show this thread](#)


Peter, in the interests of security and transparency, I ask you to please not post screenshots of my private DMs and instead publish only the information which you think people should know.

I have no recollection or record of you mailing us a hard drive and I've asked the others who were involved in the first ceremony from the Zcash Company side and they also have no such memories of records. I also don't recall any mention of it in your blog post about your participation in the ceremony. What I remember was just that you carefully protected the DVDs in tamper-evident bags for future analysis. Could you please tell us more about this mailing of a hard drive, like do you have the address you sent it to, the date, any records of communication about it?


any mention of it in your blog post about your participation in the ceremony. What I remember was just that you carefully protected the DVDs in tamper-evident bags for future analysis. Could you please tell us more about this mailing of a hard drive, like do you have the address you sent it to, the date, any records of communication about it, what kind of hard drive was it, etc?

Separately, do you still have the original discs? In order to reconstruct the transcript we need only the files off of your discs B, D, and F (plus matching files from the other five participants).

It would be good if you would send us those files or just publish them to the world yourself.

 Search Twitter

Relevant people

 **Peter Todd** @peterktodd [Follow](#)

Applied Cryptography Consultant (what the cool kids call 'blockchain tech') PGP: 0x7FAB114267E4FA04, pete@peterktodd.org

Trends for you

Trending in USA
Eugenia
25.7K Tweets

#DriveBigger
This Moon Landing Anniversary, we're helping to change the destination
Promoted by Volkswagen USA

Trending in USA
AP Rocky
Trending with: #FREEASAPROCKY, #freeASAP

US news
Trump says he will try to help ASAP Rocky, who is currently in j...

Trending in USA
#brownskingirl
42.4K Tweets

Music
Blue Ivy's vocals steal the show on ASAP Rocky, who is currently in j...

Trending in USA
#brownskingirl
42.4K Tweets

Music
Blue Ivy's vocals steal the show on

Trends for you

Trending in USA
Eugenia
25.7K Tweets

#DriveBigger
This Moon Landing Anniversary, we're helping to change the destination
Promoted by Volkswagen USA

Trending in USA
AP Rocky
Trending with: #FREEASAPROCKY, #freeASAP

US news
Trump says he will try to help ASAP Rocky, who is currently in j...

Trending in USA
#brownskingirl
42.4K Tweets

Music
Blue Ivy's vocals steal the show on

Trends for you

Trending in USA
Eugenia
25.7K Tweets

#DriveBigger
This Moon Landing Anniversary, we're helping to change the destination
Promoted by Volkswagen USA

Trending in USA
AP Rocky
Trending with: #FREEASAPROCKY, #freeASAP

US news
Trump says he will try to help ASAP Rocky, who is currently in j...

Messages

Bookmarks

Lists

Profile

More

Tweet

Messages

Bookmarks

Lists

Profile

More

Tweet

Messages

Bookmarks

Lists

Profile

More

Tweet

Messages

Bookmarks



Peter Todd
@peterktodd

Zcash has gotta be the least honest competent team in crypto.

8:53 AM · Feb 5, 2019 · Twitter for Android

15 Retweets 67 Likes



Peter Todd @peterktodd · Feb 5
Replying to @peterktodd

Also, their story that the transcript was hardly downloaded shows how right my criticisms of the lack of auditing was: basically no one had actually checked that the ceremony was correct which they refuted multiple times.

For instance the "deterministic" build broke ~1mth after.

4 3 34



Peter Todd @peterktodd · Feb 5

Really frustrating thing about this for me personally is I've been told privately by a few people that members of the Zcash team had been telling people in the cryptography community behind my back that I was incompetent and lying about the lack of auditing of the MPC, etc.

1 4 28



Peter Todd @peterktodd · Feb 5

Assuming that's true, the most charitable explanation is that they were wrecking my reputation for their cover story; the least charitable is they're happy to lie about their critics. Nasty bunch of people either way.

2 1 24



Peter Todd @peterktodd · Feb 5

I was pointed towards a bit of public corroboration, e.g. Matthew Green liking this dumb tweet: [twitter.com/el33th4xor/sta...](https://twitter.com/el33th4xor/status...)

By itself of that's pretty harmless and easily forgiven, but in conjunction with other claims and everything else, more productive to stop dealing with them.

This Tweet is unavailable.

2 14



Peter Todd @peterktodd · Feb 5

Screenshot because Emin has blocked half of crypto. :)



Emin Gün Sirer
@el33th4xor

Replying to @matthew_d_green

I can't wait to read the 28+ page drivel from a certain someone on how ZCash is broken because jellyfish are predictable, and how you have to prop your door with a chair at night.

9:57 AM · Nov 13, 2018 · Twitter for Android

3 2 64



Kill Signal @killsignal · Feb 5

Replying to @peterktodd
team > company

do honest companies even exist?

1 2



Krave.Derp.Help @skankadelika · Feb 5

Replying to @peterktodd

@snowden praising them for fixing it all thanks to the founders fee. Is he zcash shill or what? 🤔

1 2



Peter Todd @peterktodd · Feb 5

Hey, Snowden's got a decent argument there, and while team have been dishonest on occasion, the tech is genuinely good even with vulnerabilities.

Main issue is investing in Zcash carries a big risk of loss.

1 3 12



Peter Todd @peterktodd · Feb 5

Great example of how hard it is to audit Zcash.

Simple truth is Bitcoin is much simpler, and a lot less risky.

Trending in USA

#brownskingirl

42.4K Tweets

Music

Blue Ivy's vocals steal the show on



Trends for you

Trending in USA

Eugenia

25.7K Tweets

#DriveBigger

This Moon Landing Anniversary, we're helping to change the destination

Promoted by Volkswagen USA

Trending in USA

AP Rocky

Trending with: #FREEASAPROCKY, #freeASAP

US news

Trump says he will try to help A\$AP Rocky, who is currently in j...



Trending in USA

#brownskingirl

42.4K Tweets

Music

Blue Ivy's vocals steal the show on



Trends for you

Trending in USA

Eugenia

25.7K Tweets

#DriveBigger

This Moon Landing Anniversary, we're helping to change the destination

Promoted by Volkswagen USA

Trending in USA

AP Rocky

Trending with: #FREEASAPROCKY, #freeASAP

US news

Trump says he will try to help A\$AP Rocky, who is currently in j...



Trending in USA

#brownskingirl

42.4K Tweets

Music

Blue Ivy's vocals steal the show on



Trends for you

Trending in USA

Eugenia

25.7K Tweets

#DriveBigger

This Moon Landing Anniversary, we're helping to change the destination

Promoted by Volkswagen USA

Trending in USA

AP Rocky

Trending with: #FREEASAPROCKY, #freeASAP

US news

Trump says he will try to help A\$AP Rocky, who is currently in j...



Trending in USA

#brownskingirl

42.4K Tweets

Music

Blue Ivy's vocals steal the show on



Trends for you

Trending in USA

Eugenia

25.7K Tweets

Lists

Profile

More

Tweet

More

Tweet

**zooko**
@zooko

Here's what the mistake looked like in the 2013 science paper:

(a) Key generator G

- INPUTS: circuit $C: \mathbb{F}_r^n \times \mathbb{F}_r^h \rightarrow \mathbb{F}_r^l$
- OUTPUTS: proving key pk and verification key vk

1. Compute $(\tilde{A}, \tilde{B}, \tilde{C}, Z) := \text{OAPInst}(C)$: extend $\tilde{A}, \tilde{B}, \tilde{C}$ via



2



4

**Chris** @WarmindX · Feb 5

Replying to @peterktodd

peter "todd" the fud master

**CryptoNT** @CryptoN_T · Feb 5

Replying to @peterktodd

Careful zooko blocked me for such blasphemy

**#DriveBigger**

This Moon Landing Anniversary, we're helping to change the destination

Promoted by Volkswagen USA

Trending in USA

AP Rocky

Trending with: #FREEASAPROCKY, #freeASAP

US news

Trump says he will try to help ASAP Rocky, who is currently in j...



Trending in USA

#brownskingirl

42.4K Tweets

Music

Blue Ivy's vocals steal the show on Brown Skin Girl along with WizKid



Trending in USA

Sproles

Trending with: Darren Sproles

[Show more](#)

[Terms](#) [Privacy policy](#) [Cookies](#) [Ads info](#) [More](#)

© 2019 Twitter, Inc.