

Forum:[Hack Forums](#)

Thread: [Constant-Time RFC 4648 \(Base64, Base32, Base16\) Encoding](#)

sarciszewski - March 14, 2016, 9:12 am

[Available on GitHub](#).

Background

[RFC 4648](#) is an internet standard defined by the Internet Engineering Task Force (IETF) that specifies various ways to encode binary data for use in non-binary-safe transmissions; e.g. email.

These encoding schemes are useful for building cryptography features, especially when you need to store cryptographic key material in a configuration file (e.g. config.json).

However, the way these functions are normally implemented [use table look-ups indexed by the data you are encoding](#).

So I wrote (and am releasing) a PHP implementation of RFC 4648 that performs encoding and decoding in constant-time (i.e. side-steps cache-timing attacks).

Sakuto - March 14, 2016, 9:22 am

They are some strange part in your code, like this:

https://github.com/paragonie/constant_time_encoding/blob/master/src/Base32.php#L25

But thanks for this share :)

sarciszewski - March 14, 2016, 9:28 am

(Mar 14, 2016 09:22 AM)Sakuto Wrote: [\[CITE\]](#) They are some strange part in your code, like this:

https://github.com/paragonie/constant_time_encoding/blob/master/src/Base32.php#L25

But thanks for this share :)

Yeah, 7 in binary is 0000 0111.

([whatever] & 0000111) will result in a number between 0 and 7. If it equals 0, then we know we're padded properly, so we remove = characters until we run out of ='s.

After that check, if (length & 7) is not 0, then the message is invalid.

Sakuto - March 14, 2016, 10:09 am

You know that you could just do it in a loop? Same for the \$c1 = static::decode5Bits(\$chunk[2]);, use loop with array instead of repeated code.

Your project is good but it could be optimized I think :)

sarciszewski - March 14, 2016, 10:12 am

(Mar 14, 2016 10:09 AM)Sakuto Wrote: [\[CITE\]](#) You know that you could just do it in a loop? Same for the \$c1 = static::decode5Bits(\$chunk[2]);, use loop with array instead of repeated code.

Your project is good but it could be optimized I think :)

I would be wary of optimizations that could lead to execution taking a variable amount of time.

Sakuto - March 14, 2016, 10:15 am

Best thing actually is to try, if your unit test are properly written, we'll quickly figure out if it's changing anything :)

sarciszewski - March 14, 2016, 10:34 am

(Mar 14, 2016 10:15 AM)Sakuto Wrote: [\[CITE\]](#) Best thing actually is to try, if your unit test are properly written, we'll quickly figure out if it's changing anything :)

The tests don't test for nanosecond-scale time differences. :\

Sakuto - March 14, 2016, 10:58 am

I've to admit that I don't know exactly the method used in your script, I'll read some paper on it, make my test and check if optimization can be made or not. Nice share by the way

sarciszewski - March 18, 2016, 5:49 pm

(Mar 14, 2016 10:58 AM)Sakuto Wrote: [\[CITE\]](#) I've to admit that I don't know exactly the method used in your script, I'll read some paper on it, make my test and check if optimization can be made or not. Nice share by the way

Thanks. I'm not sure what papers would be relevant, except perhaps a logic table and the RFC, but feel free to suggest changes.