It seems that secure messaging projects are all the rage right now. Heck, Matthew Green is [writing about it](http://www.newyorker.com/online/blogs/elements/2013/11/the-daunting-challenge-of-secure-e-mail.html) in the New Yorker this week!

[One of my side-projects](https://pond.imperialviolet.org/) for a year or so has been about secure messaging. Of course, that means that I was working on it *before* it was cool (insert hipster emoticon here, :{D ) … but I'm slow because my side projects get very little time. (When I started, the subheading for the project was “How to better organise a discreet relationship with the Director of the CIA”, because that was the topical reference at the time. Oh, how things change.)

It's still not really ready, but the one year mark seemed like a good deadline to give myself to mention it in public. You should pay heed to the warning on the project page however. I did contact one, well known, security auditing company to see whether they would take a couple thousand dollars to spend a day on it, but they said that don't really do small projects and that I'd need to be talking 10-20 times that for a couple of weeks at least. So don't depend on it yet and don't be surprised if I've just broken it somehow by replacing the ratchet code. (Although, thanks, Trevor, for the design.)

But I fear that it's not going to make Matthew Green happy! It's certainly not a drop-in replacement for email. I spend my days working on small changes with a large multiplier, in my free time I choose to shift the balance completely the other way.

* *Ephemeral messages*: although no software can prevent a recipient from making a copy of a message, it's the social norm and technical default in [Pond](https://pond.imperialviolet.org/) that messages are erased after a week.
* *No spam*: only approved contacts can send you messages. In order for the server to enforce that without revealing the identity of every sender, pairing-based, group signatures are used. (The flip side is that there are no public addresses, so you can't message someone that you don't already know.)
* *Forward security*: the exchange of messages drives a Diffie-Hellman ratchet preventing a point-in-time compromise from giving the attacker the ability to decrypt past messages (modulo the week-long retention).
* *Erasure storage*: since B-tree filesystems like btrfs and log-structured SSDs mean that one can have very little confidence in being able to securely erase anything, [Pond](https://pond.imperialviolet.org/) tries to use the TPM NVRAM to securely delete old state. (Note: not implemented for OS X yet.)
* *One-to-one only*: No messages to multiple contacts (yet). Haven't implemented it.

The source code is in Go, but there are binaries for several Linux flavors and OS X. (Although it looks terrible on OS X and one user reports that the program can only be closed by killing it from the command line: I've not reproduced that yet.) In addition to the default server, I learned recently that the Wau Holland Foundation [also runs a Pond server](http://www.wauland.de/en/index.html).

For more details, see the [user guide](https://pond.imperialviolet.org/user.html), [threat model](https://pond.imperialviolet.org/threat.html) etc which are linked from the [project page](https://pond.imperialviolet.org/).

If you get it running, but don't know anyone else, you can use:

gpg --recv-key C92172384F387DBAED4D420165EB9636F02C5704

to get my public key and email me a shared-secret. (Although I only check that email during the evenings.)