Encrypted Authorship

Nemo Niktov
nemo.niktov@protonmail.com

Abstract. This paper proposes *encrypted authorship* as an alternative to anonymity and pseudonimity. The method is simple and relies only on standard cryptography tools that can be easily used by anyone.

There are many reasons why authors might want to publish their works without revealing who they are. And there are also reasons why society should allow, and even encourage them to do so.

One of the most prominent reasons is to avoid subjective, preconceived and often unconscious discrimination. Scientific works ought to be evaluated objectively, and it is well-known that an author's gender, country of origin, affiliation and status within a scientific field may bias the evaluation.

Another crucial reason for seeking and allowing publication without revealing authorship is to avoid censorship of various kinds. Scientists need to be able to publish results that are against the interests of their employers, the ideologies of their country's government of his country, or even their academic communities, without jeopardizing their jobs, their safety, their careers and their reputation.

The most trivial way not to reveal authorship is to publish anonymously. However, this solution has disadvantages. The authors, whose careers often depend on being able to show that they have produced high-impact publications, are incapable of proving the anonymous work is theirs. And society cannot hold anyone accountable for an anonymous work. The lack of accountability is presumably why conferences and journals prohibit anonymous publications.

Double blind reviewing is a form of temporary anonymity, lasting only during the reviewing process. However, the issues reappear when papers are published and the authors are revealed. It is not only during peer review that papers may be judged in a biased manner. Even after publication, papers continue to be evaluated. A potential reader's decision to read or not to read a paper, and to cite or not to cite it, may be influenced by available information about the authors. Moreover, because a new paper typically is an extension of, or relates to, previous published papers of the same authors, double blind reviewing often simply does not work, because reviewers may easily guess who wrote the new paper, especially when the community is small. The effectiveness of double blind reviewing is further jeopardized by the culture of irreversibly posting non-anonymous preprints in servers such as arXiv.

Some authors have preferred to hide their identities not through anonymity but by using pseudonyms. A pseudonym allows authors to easily circumvent policies that prohibit anonymous publication. Even if the policies also prohibit pseudonyms, it may be difficult for the editors to suspect that a given name

is actually a pseudonym. Pseudonymity is more powerful against biases than anonymity, because authors may choose a positively biased name.

It is still impossible for an author to provably claim credit for works published under pseudonyms. Some authors have attempted to circumvent this limitation by choosing pseudonyms that are related to their real names. For instance, the pseudonym may be an anagram of the real name or a rough translation of the real name into another language. However, such approaches do not provide reliable proofs of authorship and they make it easier to guess the real name of the author.

Nowadays, thanks to widely available cryptography tools (e.g. GPG – GNU Privacy Guard), it is possible to define a simple method that can be used to:

1. Ensure that an author's real name remains secret.
2. Let the author's real name be known to a chosen subset of stakeholders (e.g. funding agencies and employers interested in measuring the author's productivity, or authorities responsible for ensuring accountability).
3. Allow the author to privately prove authorship to anyone.

The idea is simple: the authors publish the paper using pseudonyms and include their real names, their affiliations and any other identifying information as encrypted signed messages at the end of the paper. This can be done according to the following steps:

1. Create an email address for the real name, in case it does not yet exist.
2. Generate a private key and a public key for the real name.
3. Invent a pseudonym.
4. Create an email address for the pseudonym.
5. Generate a private key and a public key for the pseudonym.
6. Write the real name and any other identifying information (e.g. affiliation) in a text and sign it using the real name's private key. This generates a clear text signature that contains both the real name and the signature.
7. Obtain public keys of stakeholders (e.g. editors, funding agencies, employers).
8. Encrypt the signed clear text using the public keys of the pseudonym and the stakeholders and sign it using the pseudonym's private key.
9. Include the encrypted message at the end of the paper.

Now the stakeholders can know the real name of the author by decrypting the message. If in the future the author would like to prove authorship to people who are not among the pre-selected stakeholders, the author may meet them privately and decrypt the message in front of them. A more drastic option, if the author would be willing to permanently reveal his real name to everyone, would be to publicly share the pseudonym's private key (and revoke it). Then anyone holding the private key would be able to decrypt the message.

```
-----BEGIN PGP MESSAGE-----

hQEMAxGcuKeZO3sjAQf/flNISMMal8HCQS12hq+j9Mxj+f+mIf2cPOHcDIvkke4x
dsbTt8OxgWbiVCWBfFr8+BmDi+f1jPojgspwCKnrYHHOhpMTqqo4Di8Gm+P/3pH5
7LhL3I6rmhi/DujDQ5+eXhVy7aYFGrKGS/p+tGOZiyqYB/GDbh1jOdaBgelTzdLC
CcmZwLEtLrPzo9JydRSXx+NUy+Ya1jBap4hY8UrJsyBkYmf0Oe5EMwKnvfS38RKC
IGg5FD6PcHIJOm7ePiGBwmeRkMx6Mu+7Ml+mZMj3ILU27EgLDy/ONBe9LMSIALKJ
OKUUnW9yJUkd+ODNR6dJ/jm5h+gXPsOERNNzuJMzXdLqAcs5DKE9PYGvZx8Osmwo
wcQlEOm3rH5QNlRLrUSZ722LkjJIbV55Cu94rOzxPjwfKbUtBuhfaRjqhXOPbUU3
UMdLluwWrVBvW2kOyZuFslxVh22AZeA0kU5Oq6hjPFLfZ1nZfYX3NpOqqur2jCeV
X1JBGIv5NG4jQfm2HUChlB6Oq75955otA6xBKLIhjFfx3SSM2UhhlxAR8WNFSbz1
QbODLhtcZkJbQl9i+xJNV5GeL4oGtuIkWSBkAsNOOXMQSrHMd915sLtrwyFTXhr8
a2uzuGq7MGLrQ2WQG0gOCTEFX8Byg92w8+8uunRXM9GKiGbz615HBjFPCOAnQVyu
rScEjHeVLlCJdpJeVoEsxCaTLgYzvZnKA4ZUylMFCfjwBesUz3Lape07WPG7RE9x
g1vmL39X9qUJpOUP+sw8l4RWxN5oSP2gFBd23/WcwfhH3i/NPyN12S5Qq7k291YV
2ANlgy6YPpbQG1tL1aKKiVJdd6n0ZNoCP7krCT+DBoShlh1UC2hd4tyqgUekB4WB
wypfOnS3fqv0YDj2Vj4PO/DBUPdOq6dxy8tADus+V+/1I+Am1bpyy7ILtfUYZd9w
kPYtf9G9Hv+js55IMc4sBjcVb4D5Oq6cX6VBZtYIGmOojBSigM1qJFa6qt3qlSy6
q+Fe3x2r/vqFvU6P+v+ncKrMgF9O62WB1W6NY+geZOEvkjFeCPizOFLt5WGKzafp
v51oOE8tSr4vgtcDyN+cODh/BNryzIcm36JwzkuGnPvGATiOR6ZA3Xqb14anyX6y
ihwHJRbPthF4urnAXjaKtZ+vM2MUvlG3o4YTMphGiSnGSyy32I4sByYaDgLeyPSJ
tWSvScKUfVRmrVAnd5rtlpLyVSt1e7vkGjZGZfMKX80jPQ9ICdNtMCXh5ZQBy0/6
/SdumxROFOQTFHFa9eVRLY+V6PzNWRUAGK8QyNRTtvJpY1diq1wsuXkWP1aubZrf
ved6Ppbw6URbPsI1NbZYF+eH6uqtqp3k4+fEdIUbellcA8aKJ9wbcGk+h92jfrKA
SzeicWydjx+fnMesTM4I85zo/O9x3iRpkFAL6Zb9qObiVuwIS/315TY1DN3FT7ec
6I3x12A7Gg1k/U3vt7u8/73UOJUp5ScDXHNtsCCMwzRsbNTlX88CMqcPbS3oUUt0
xbmdanQy8yOSb0lZnf6lJJTDb76+Iax/YWx5DjdEmbuHhNYbuzj7QB5du7qQC4mA
3W4CotfXgta7bz7qH/kUa7Upxc5IZmxUOSNfLFpkncgw3EAq80DdyG9Qo5euaQpL
sE18sEUJawwsPXdevc/JZekbIdLGq0/jvKsXbFumJm8Rfr7R6KmLVo3f1Hb3br/L
lKFRBu/rY3HwNdjirx50HdEyFQm7g+n3rphhjrCcyU2kYUZ5KrFOcVG7JIfbK6zN
RcoyyhMD2UWS86zDn1nl9TP7FPT1tEWwMBChEUtCgCOeVCL31OyWris/HzpboAON
d/5hoB7WvXAt2cM3HHx6Q0mxyEgM7T4V++sQasPpW5vZJy2ogJd3/Fc1tGyeNXdH
w8/Q10k3NLb9NI1zB7JOVct9oA==
=DEQY
-----END PGP MESSAGE-----
```