Dining Cryptographers’ Wiki
IMPLEMENTATION SUMMARY

Immanuel Scholz
Technische Universität Dresden
immanuel.scholz@tu-dresden.de

Abstract. This paper introduces an implementation of a closed group distributed anonymous wiki based on a Dining Cryptographer (DC) network. We argue that such a wiki application particularly suits the properties of a DC network, e.g., performance is less important, and broadcast communication is needed by default.

1 Introduction

Dining Cryptographer networks have been known for more than 20 years [1]. However, there exist few to none implementations, largely because the performance of DC networks was considered as insufficient for general purpose anonymous communication. Alternative protocols, such as MIX networks, require less overhead for bilateral anonymous communications.

Even though DC networks provide some features not available in other protocols for anonymous communication, for example

– asynchronous submits of message content,
– broadcast by default,
– higher robustness against data retention than MIX cascades,
– possibility to achieve unconditional anonymity [2].

Probably the main reason for the lack of widespread implementations of DC networks is its comparatively high bandwidth overhead in typically bilateral communication. Also, the set of participants in a DC network is assumed to be fixed and we are not aware of rigorous analyses of the consequences of dynamic joining or leaving.

However, by choosing the right scenario, most of the disadvantages of DC networks are less important and their advantages come to play.

The objective of this paper is not a comprehensive theoretical discussion, but rather a supporting document for a concrete implementation to be presented to the HotPETs audience.

2 Principles of the DC network

A DC network consists of a set of participants that have mutually agreed on a secret and send messages to each other in every round. All round messages are
summed together and the result is the message content sent by one of the participants. The sender is not identifiable in the set of participants (sender anonymity). Since the message content is broadcasted, all participants are receivers (receiver anonymity). Extensions to this basic scheme that allow the protection against faults or malicious participants have been proposed in the literature [3].

3 The DCWiki

In this section we briefly describe the architecture of an anonymous wiki based on DC networks as well as details of its current state of the implementation. A wiki is a distributed application for collaborative content creation and sharing.

The main idea is to realise a wiki communication protocol over a DC network. We therefore distinguish between three different types of data:

- **Wiki content** is the shared content of the wiki, typically human-readable text, which is created and edited collaboratively by all participants.
- **Message content** is the content of the single message broadcasted in a DC network round, typically editing information. The combination of all message contents yields the wiki content.
- **Round message** is a message published by an individual participant. A single round message is indistinguishable from random bits. The sum of all round messages in one round yields the message content of the round.

In the following we elaborate on the design decisions for our concrete implementation as well as technical details thereof.

3.1 Design decisions

The network is organised fully decentralised with symmetric task sharing, i.e. there are no participants or ‘servers’ with special functions [4]. The only requirement a user needs to participate in the DCWiki is a place to publish arbitrary data.\(^1\)

This data are individual DC round messages. Fig. 1 visualises this DC network layer of communication. In the static case, a list of participants and their respective publishing site has to be shared beforehand. Extensions for dynamic joining and leaving are conceivable but not detailed here for brevity. Note that the publishing sites do not need to know each other.

When a user edits the wiki, a round message containing the content differences is built and prepared to be published in a future DC round. In fact, this can be done offline. Once a connection to the Internet is established, the pending DC rounds are uploaded to the own publishing site and all other participants’ published round messages are downloaded. When all round messages are collected,

\(^1\) As the data is indistinguishable from random numbers, publishing random data has to be compliant with local authorities. Otherwise steganographic methods could be used to circumvent this restriction.
each participant locally sums them up and the resulting message contents are incorporated in the current wiki content.

Note that in theory, anybody who knows all publishing sites can recover the broadcasted wiki content and re-distribute it to a wider audience. This could be useful for human rights NGOs or independent media organisations who ‘leak’ anonymously aggregated information to the public.

Unconditional anonymity is optional, but requires secure exchange of symmetric one-time pads between the participants. Mind that, unlike for many other scenarios, this is not so unrealistic in a closed group of participants. It is even possible to combine it with conditionally secure key exchanges: paranoid participants can form subsets and share one-time pads.

To highlight the advantages of our approach, Table 1 contrasts the difference between DCWiki and an imaginary anonymous wiki application referred to as “MIX-wiki”. The MIX-wiki is thought to be a combination of a standard wiki hosted on a central server, and a low latency web anonymiser (e.g., JAP\(^2\) or Tor\(^3\)). Of course, more elaborate solutions with MIX networks are conceivable but would require a special implementation as well.

### 3.2 Implementation details

The DCWiki software to be presented contains a Java service for the communication part that runs locally on each participant’s computer and implements some features of what is known as DC\(^+\) network [2]. The current state of the implementation is based on a DC chat application demonstrator [5].

Participants can be identified by either their GnuPG\(^4\) key or a random number generated when registering in the DC network.\(^5\) The GnuPG web of trust is used to secure the mutual key exchange using a Diffie-Hellman protocol [6]. As a result, the achievable anonymity is only conditionally secure.

Our DCWiki software contains a simple self-made wiki running as local web server and accepting page edits. Replacing the generic wiki with the common MediaWiki\(^6\) is envisaged. The edits are broadcasted through the Java DCWiki component and received differences are applied automatically.

### 4 Related work

The closest concrete implementations to our system we are aware of include the FreeHaven project [7] and a case study on covert collaboration [8]. The former uses secret sharing techniques to distribute static content in a censor-resistant

\(^2\) [http://anon.inf.tu-dresden.de](http://anon.inf.tu-dresden.de)

\(^3\) [http://www.torproject.org](http://www.torproject.org)

\(^4\) [http://www.gnupg.org](http://www.gnupg.org)

\(^5\) This does not compromise anonymity. Like many other anonymity networks, DC is only protecting who of the participants is sending, not who is a participant.

\(^6\) [http://www.mediawiki.org](http://www.mediawiki.org)
way. The latter embeds the protocol for a wiki application in an image sharing
service, but does not guarantee anonymity of the participants.

We are grateful to receive pointers to further closely related projects from
the HotPETs participants.

5 Presentation

The aim of this HotPETs submission is to present and discuss our DCWiki
application. The audience will be invited to join a demonstration DCWiki right
on the symposium. So the speaker can be criticised fully anonymously.

Acknowledgements

The author thanks the TU Dresden coffee party (the members of which prefer
to remain anonymous), especially Rainer Böhme and Stefan Köpsell . . .

References

2. Waidner, M., Pfitzmann, B.: Unconditional sender and recipient untraceability in
3. Waidner, M., Pfitzmann, B.: The dining cryptographers in the disco - undercondi-
tional sender and recipient untraceability with computationally secure serviceability
(abstract). In: EUROCRYPT. (1989) 690
panel “Mix cascades versus peer-to-peer: Is one concept superior?” . In Martin, D.,
243–255
5. Scholz, I.: Dining cryptographers, the protocol. In: 24th Chaos Communication
Congress. (2007)
Information Theory 22 (1976) 644–654
anonymous storage service. In Federrath, H., ed.: Workshop on Design Issues in
Table 1. Comparison of Wiki based on DC and MIX networks

<table>
<thead>
<tr>
<th>Aspect</th>
<th>DCWiki</th>
<th>MIX-wiki</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure dependence</td>
<td>arbitrary publishing site</td>
<td>interconnected MIX servers</td>
</tr>
<tr>
<td>Distributed storage of the data?</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Who has to cooperate for successful data retention?</td>
<td>all participants</td>
<td>all participants or all MIX servers</td>
</tr>
<tr>
<td>Robust against intersection attacks? a)</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Dynamic joining/leaving of participants?</td>
<td>limited</td>
<td>yes</td>
</tr>
<tr>
<td>Possibility to hide the entire service?</td>
<td>yes</td>
<td>limited b)</td>
</tr>
<tr>
<td>Unconditional anonymity possible?</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

a) in the absence of dummy traffic
b) the fact that a MIX network is used remains observable

Fig. 1. Information flow in the DC network layer of the DCWiki application