CoverTagDrop: Efficient Dead Drop Decryption with Bloom Filters

Michael C. Fink Amores
University of Cambridge
mcf61@cam.ac.uk

Daniel Hugenroth
University of Cambridge
dh623@cam.ac.uk

Alastair R. Beresford
University of Cambridge
arb33@cam.ac.uk

Whistleblowing requires secure communication channels that protect disclosures made in the public interest, as recognized by legal frameworks such as the *Public Interest Disclosure Act 1998*. To address this need, *CoverDrop* [2] provides strong metadata security for end-to-end encrypted communication between whistleblowers and journalists via the Guardian mobile application. Recently deployed by *The Guardian* in collaboration with the *University of Cambridge*, the system is designed to mitigate the first-contact problem and to offer stronger metadata protection than conventional end-to-end encrypted messaging platforms. Messages are sent to a centralized *CoverNode*, which aggregates messages from all clients, mixes them to hide their origin, and releases them in fixed-size groups called *dead drops*. Clients periodically download these batches of encrypted messages via a public API. To obscure communication patterns, all client devices regularly send dummy messages that are indistinguishable from genuine messages but contain no meaningful content, even when no real communication is taking place. CoverDrop adopts an asymmetric communication model that distinguishes between journalists and regular users with different roles and privileges.

To ensure forward security, CoverDrop employs frequent rotation of public messaging keys. In the system's asynchronous, high-latency setting, messages may therefore be encrypted under keys that are no longer current at the time of retrieval. As a result, a receiving client cannot assume which key was used and must instead consider multiple, potentially older, keys when searching for intended messages. Since all messages within a dead drop are indistinguishable at retrieval time, this forces the client to rely on exhaustive *trial(-and-error) decryption*. To preserve plausible deniability, dead drops are decrypted only when a client explicitly unlocks a CoverDrop session, rather than continuously in the background. Consequently, decryption is performed intermittently and in concentrated bursts. The overall cost of dead drop decryption is driven by two factors: message throughput, determined by the number and size of retrieved dead drops, and the cost of decrypting an individual message, which depends on the number of candidate key combinations that must be evaluated during trial decryption. Looking ahead, it is reasonable to expect that additional news organisations, both within the United Kingdom and internationally, will adopt CoverDrop as part of their mobile applications. Further strengthening metadata privacy may also require unifying deployments into a single, geographically independent mix network. Both developments would increase message throughput and thereby amplify decryption costs. At the same time, per-message decryption costs are likely to rise as the protocol evolves. While the current system relies primarily on elliptic-curve-based primitives provided by *libsodium*, an anticipated transition to post-quantum cryptography would introduce higher computational, memory, and bandwidth requirements. Together, these factors make large-scale trial decryption over dead drops particularly expensive for mobile devices, where increased computation directly translates into higher energy consumption and reduced battery life.

We introduce *CoverTagDrop*, an extension to CoverDrop that significantly improves the efficiency of message retrieval from dead drops by enabling clients to identify candidate messages prior to decryption. Our approach uses one-way hash functions to derive short plaintext identifiers from shared session secrets and the public keys used for encryption, which are appended to messages and allow clients to efficiently scan dead drops for matches. The underlying session secrets evolve over time in a manner analogous to key updates in *Signal's Double Ratchet* [1]. Their initial establishment does not require an explicit interactive key exchange, as the initial session secret can be included in an user's first encrypted message. From the journalist's perspective, discovery of a message that initiates a new communication session is facilitated by the trusted CoverNode, which intermediates message delivery and resolves the first-contact problem. We show that decryption attempts can be reduced by up to a factor of 70 using message tags as small as 4 bits, offering a substantial gain for almost no communication overhead. Decryption costs can be reduced further by embedding Bloom filters into each dead drop, populated with hash values derived solely from the evolving session secret, enabling clients to quickly discard dead drops unlikely to contain relevant messages even when the specific public keys used for encryption are unknown and the system is dominated by dummy traffic. Both these techniques reduce the message search space and associated computational burden, improving scalability under wider adoption and better preparing the protocol for more computationally demanding cryptographic primitives.

[1] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 451–466. IEEE, 2017.

[2] Daniel Hugenroth, Sam Cutler, Dominic Kendrick, Mario Savarese, Zeke Hunter-Green, Philip McMahon, Marjan Kalanaki, Diana A. Vasile, Sabina Bejasa-Dimmock, Luke Hoyland, and Alastair R. Beresford. CoverDrop White Paper. `https://www.coverdrop.org/`, 2025.