Randomness & Time-Lock Encryption

Raphael Tannous

Applied Cryptography - Summer 2026

Randomness

What is randomness?

Is This Random?

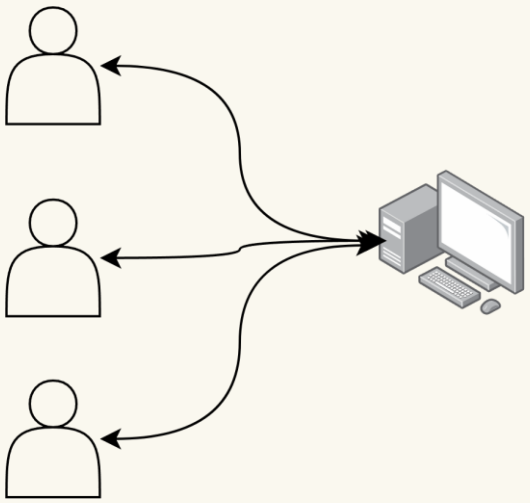
00010010 10011101 01101101 11111101	**Yes**, randomness from (/dev/urandom).
00000001 00000010 00000011 00000100	**No**, this is 1,2,3,4 in binary.
10101010 10101011 10100001 10100010	**No**, this is 0xAA, 0xAB, 0xA1, 0xA2.
00000000 00000000 00000000 00000000	**No**, All zeros.

However, each number has the same probability to occur, but true randomness is a number that lacks a pattern.

Randomness

Public randomness is important, so is private randomness.

Public Randomness



- Lottery Systems.
- Games.
- Elections.
- Timelock Encryption.

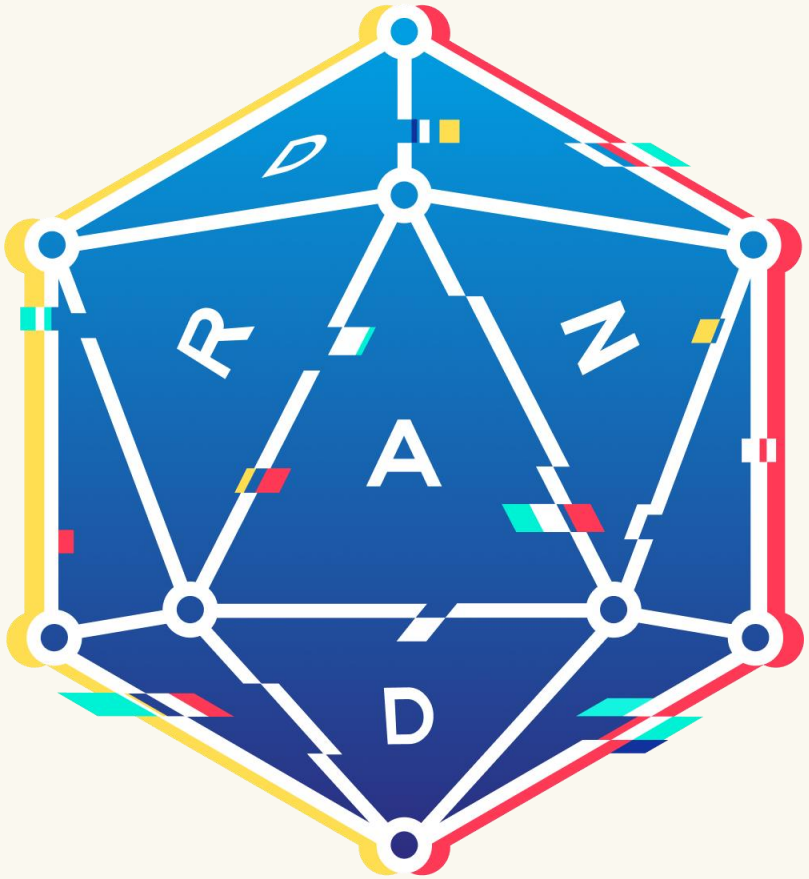
Private Randomness



- Wallet Seed Phrase.
- TLS ephemeral keys.
- Device encryption.
- Nonces.
- Zero-knowledge proofs.
- Salts.

Public Randomness Using drand

drand is a distributed network that provides bias-resistant, publicly verifiable, and unpredictable randomness.



Setup Phase

Uses DKG and each participant in the drand network will have a private key share.

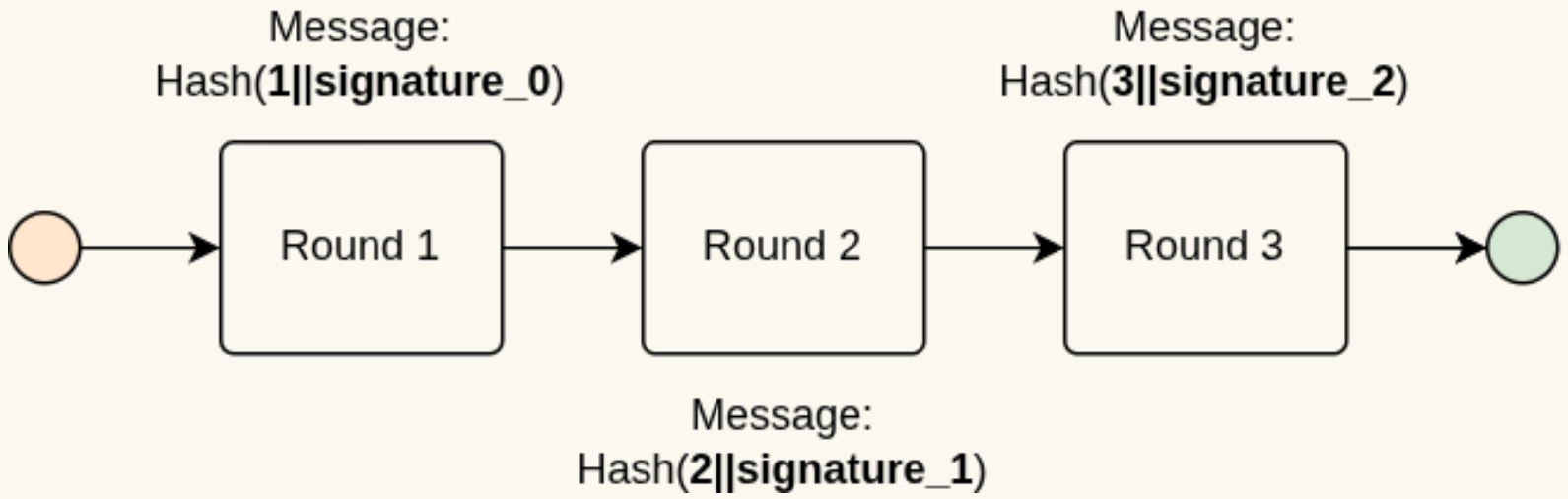
Beacon Phase

Each round, each participant takes a message (which depends on the network mode) and signs it using its own private key share using Threshold BLS signature scheme, then broadcasts the signature.

When a threshold of partial signatures is collected, anyone can aggregate them into a BLS signature that is used as randomness.

drand's Default Network

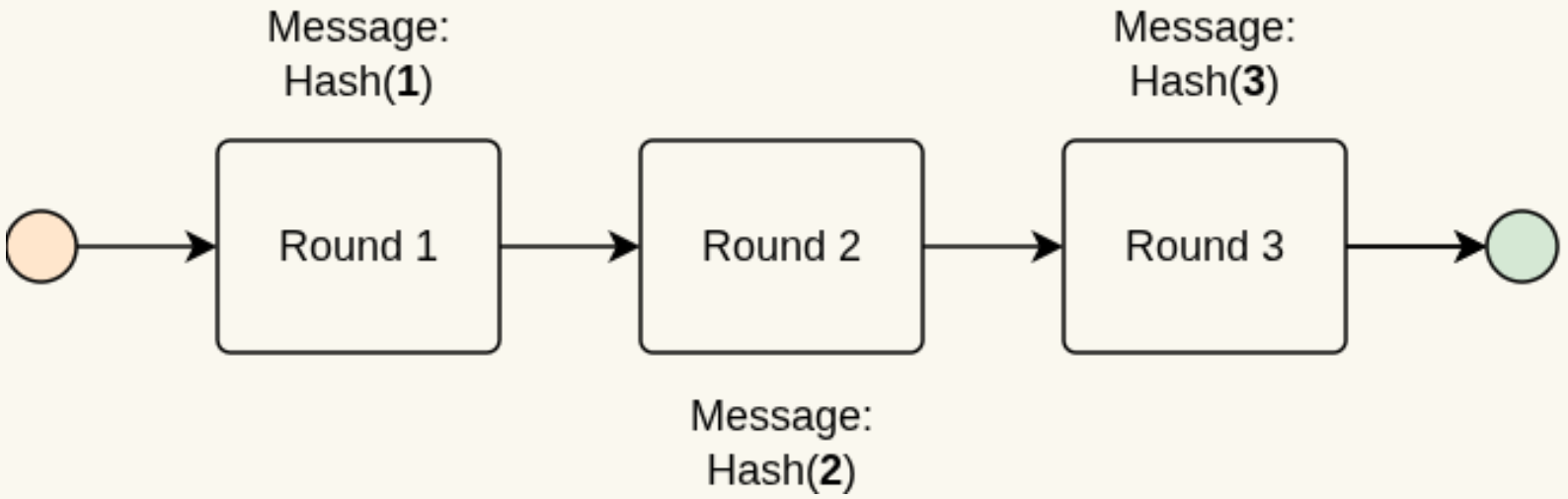
drand's default network periodically generates publicly, verifiable, bias-resistant, and unpredictable randomness. drand's default network is a chained network.




```
{
  "round": 6522645,
  "signature":
"b6b13209bfd5377974588d0666a5a9363e5f017764fa379cdb688bd3250b633941f245c8220d3e4890cd207d8694f174011831566b0cf2389189c6
cd6961deb54178dfdf9b9ae59f03ed1027d1d60bf1ba331ea077cd5da798154b5d3b619062",
  "previous_signature":
"97660b3fee2af886f96a0b862cee6de9747f9abaea9632c349f0f3331d7581724d3c43a134a74497b89c0ee533994c340412b1188c5d6945ce86dd
1c6a20803502699ff3ea5b10fa9e4a21442ed5b6b4c4f5d90e96a0fead44193929dcfd95b4"
}
```

drand's Quicknet Network

drand's quicknet network is an unchained network.




```
{
  "round": 33230871,
  "signature": "977315cfad2327d12f97a145044c6e1bc59c67c89542d5c6dad9fc282ee81faf2ee6128e8968e8c174d709ca13a77ee1"
}
```

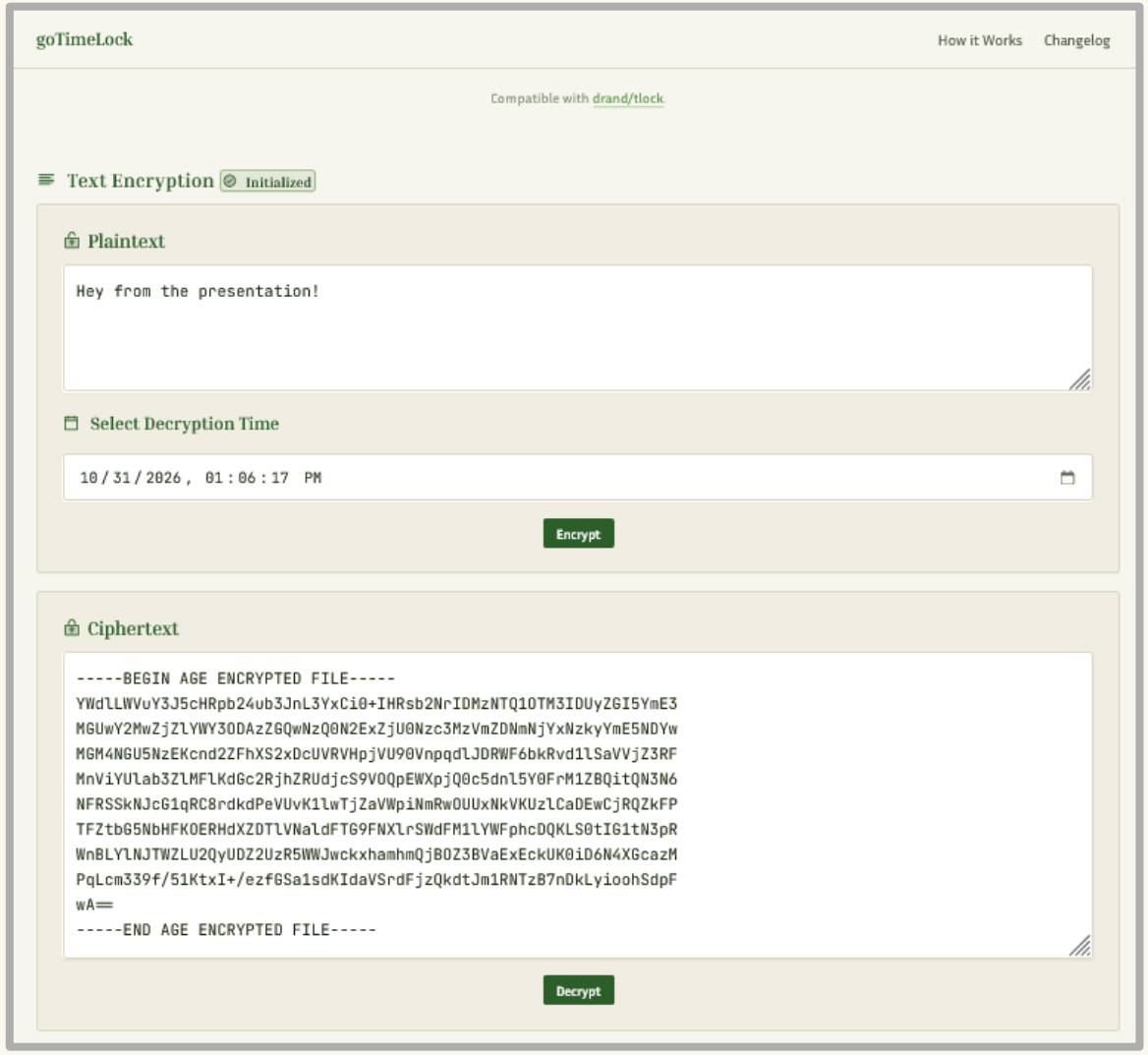
Part 1: On Randomness

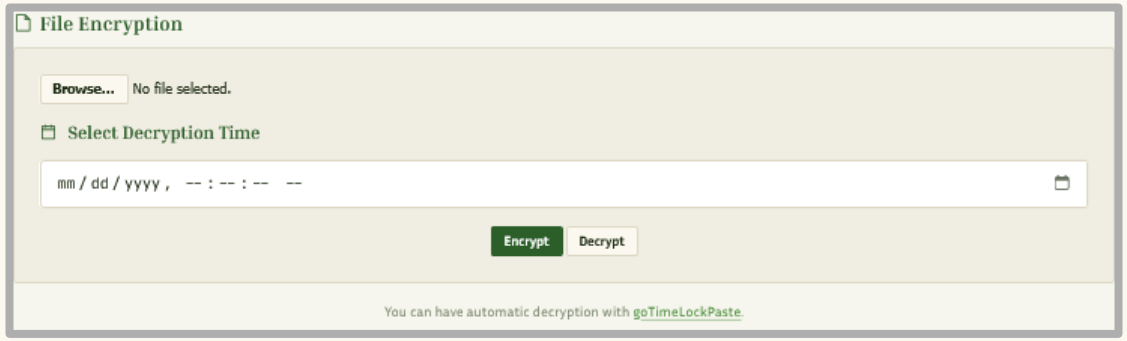
Using drand's default network we can create a LOTO system.



Part 2: On Time-Lock Encryption

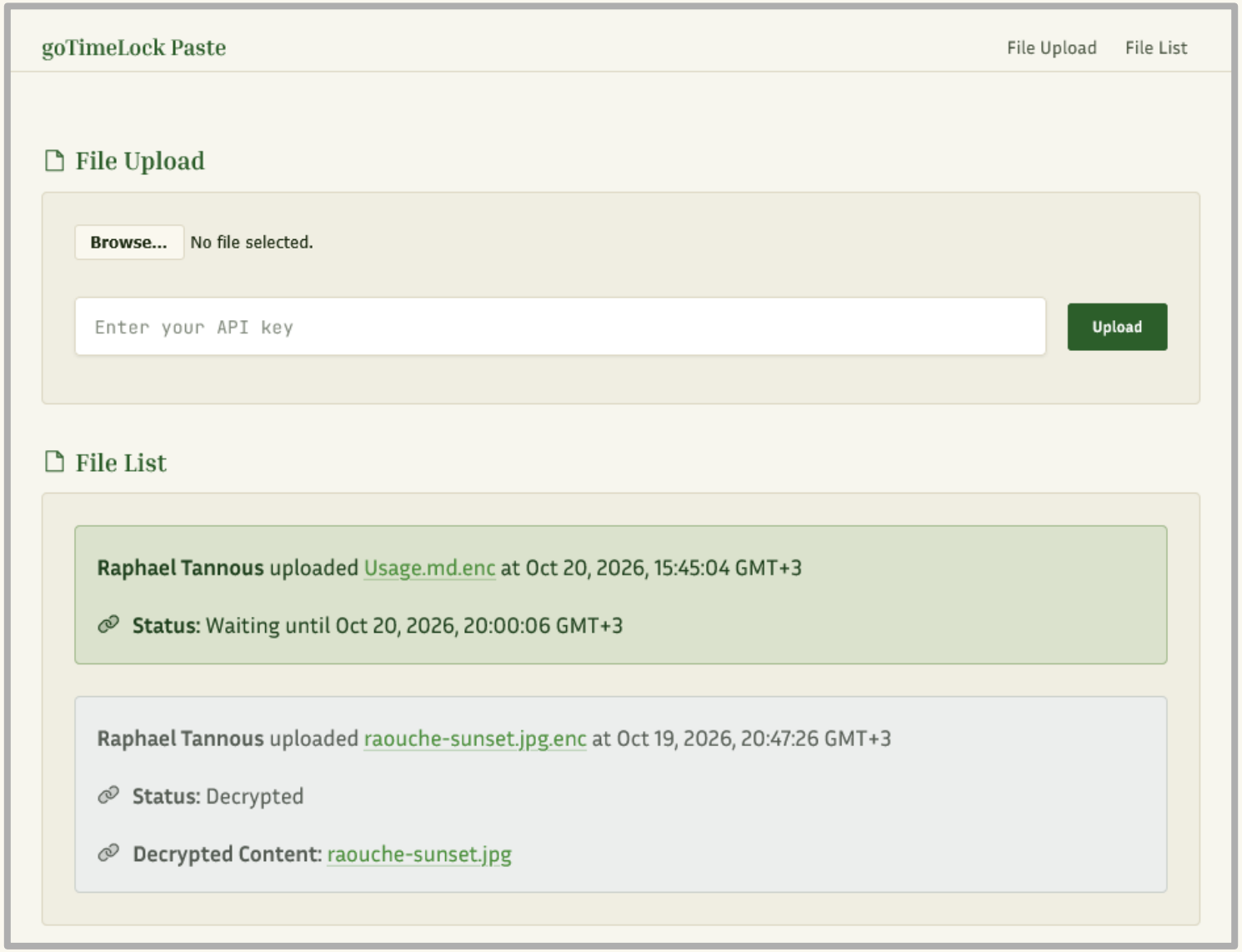
Using drand's quicknet network we can create a time-lock system.





Part 2.1: On Automatic Decryption

Having created ciphertexts we can create an automatic decryption system.



Workshop

goLOTO

goTimeLock

goTimeLockPaste

Thank You!

Any Questions?

Raphael Tannous

riyt.dev

Applied Cryptography - Summer 2026