A method to secure digital content by synthesizing digital twin using dynamic colour mapping

Rajarshi Sanyal , Ph.D. Proximus Luxembourg

Srinjoy Sanyal, University of Luxembourg

Background

- Cloud infrastructure can store sensitive and static documents.

- Example: Contents related to domains (non restrictive) of Healthcare, Finance, Legal, Cloud Computing, etc. may need a very high grade of security.

- The focus of this paper is a propose a method and system (*patent pending*) to enhance the security of static contents in cloud drives or transferred to another storage location

- During the transfer of contents, there is a perennial risk of man-in-middle attacks where the key to encrypt / decrypt can be compromised.

“State of the Art” encryption-decryption mechanisms

Hybrid Cryptography

- Combines the speed of symmetric cryptography with the security of asymmetric cryptography
- 3 keys
  - **Symmetric public key**: used to encrypt and decrypt document
  - **Asymmetric public key**: shared between users and used to encrypt symmetric public key
  - **Asymmetric private key**: not shared between users and used to decrypt symmetric public key

Zero Knowledge Proof

- The user must prove to a System (called Verifier) that a statement is correct without revealing the statement itself
- User does this by performing multiple tasks
- Stochastic method
  - There is a chance, however small it might be, that an attacker performs all the tasks correctly at random

Quantum Cryptography

- Process to encrypt / decrypt data and store or transmit secure data based on quantum uncertainty principles

Problem statement / Research Question

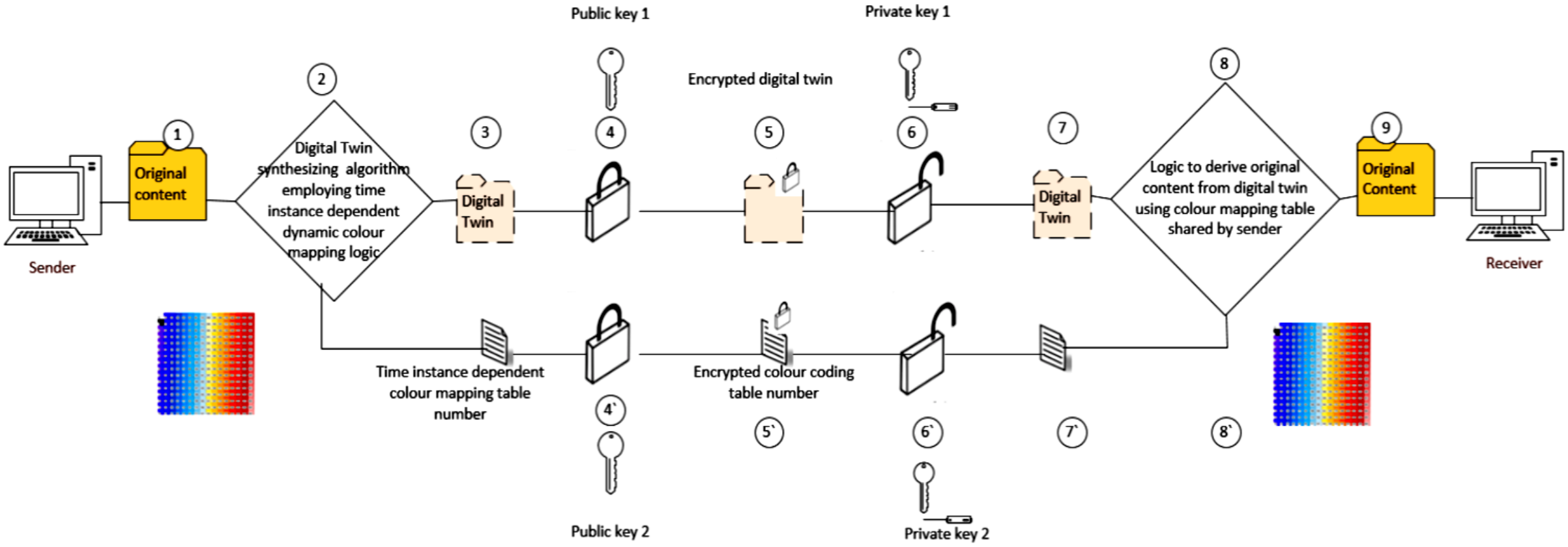
A key concern is the security of the private and the public keys themselves.

- **Public-private key encryption setup**: an attacker can pose to be a user and can gain control of the private key.
- **Public key encryption**: the chances of a security breach increase manifold as the channel to share the keys may be compromised.
- Possible performance impact due to long key size
- Attackers are relentlessly finding ways to exploit the cryptology systemsby deploying memory snapshots, DOM scraping or MITM attacks.
- Zero Knowledge Proof brings in a chance of rogue provers that may evoke `soundness error`

Research Question :**"Can we add an extra layer of security by synthesizing a digital twin using a colour mapping algorithm that uses a dynamic colour code table?"**

- Encryption performed on digital twin, not on the actual content
- Even if the encryption is cracked, it might be difficult to reconstruct the original content
    - Hacker will have to choose between millions of possible colour code tables to get the actual content

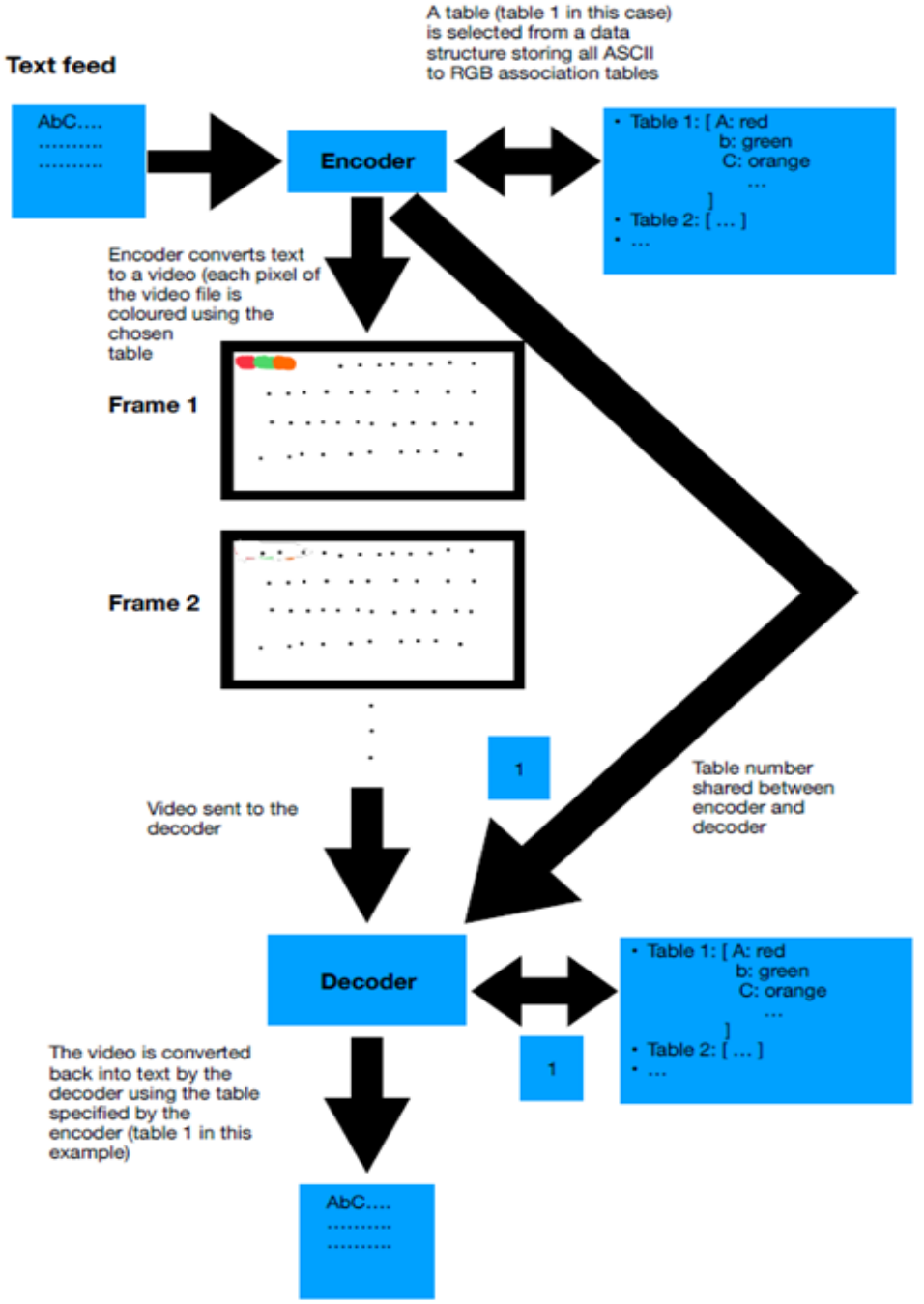
End-to-end architecture



- Digital twin created using a specific color mapping table
- Digital twin and color mapping table number shared between sender and receiver through different secure channels
- Digital twin decrypted by using table number

Digital twin creation process

- **Encoder**: Encrypts a document using a specific color mapping table
- **Decoder**: Decrypts the document by fetching the color mapping table used by the encoder
- Table number and digital twin shared securely between encoder and decoder



Conclusion and future scope

Conclusion:

- Millions to billions of possible color mapping tables to synthesize digital twin
  - Difficult for attackers to brute-force
- Different physical channels used to convey the colour mapping table number and the encrypted digital twin from sender to receiver

- **Partnership / EU Funding sought :**
  - Partner for Proof of concept
  - Penetration testing to validate the potency of the novel algorithm and comparison with “state of the art” algorithms
  - Assess regulatory constraints
  - Target: Realize as a security product for institutions / cloud providers

Research Experience

- Ph.D. Supervisor
- 30+ research publications
- 6 patents (5 granted)
- Linked to 2 EC projects in the field of 6G telecommunications