ASTRAN

NIST
National Institute of Standards and Technology

AONT: an essential gadget for Multi-Party Threshold Cryptography.

presented by Gilles Seghaier, Cofounder & CTPO of Astran
during Session 3c (13:20 EDT) Thursday, September 28th, 2023

MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023

astran.io @astran hello@astran.io

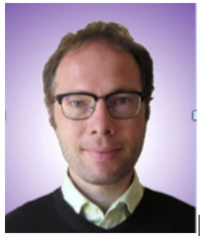
THANK YOU

NIST

Astran Academic Partners

LIP6 · CNRS · GDR Sécurité Informatique · UNIVERSITÉ DE LORRAINE · LIMOS

Astran Scientific Committee



Ludovic Perret

Nigel Smart

Professor Nigel Smart - Cryptographer and professor of computer science at the University of Leuven in Belgium, renowned for his work on elliptic curve cryptography and matching-based cryptography. He co-founded Unbound Security, a company specializing in the deployment of distributed cryptographic solutions based on multiparty computation (MPC).

Professor Ludovic Perret - Cryptography expert and lecturer at Sorbonne University, specializing in the standardization of post-quantum cryptography. Co-author of the GeMSS digital signature scheme and involved in several standardization bodies.

Zero Trust & Zero Knowledge Cloud Services

aws S3

Simple
Storage
Service

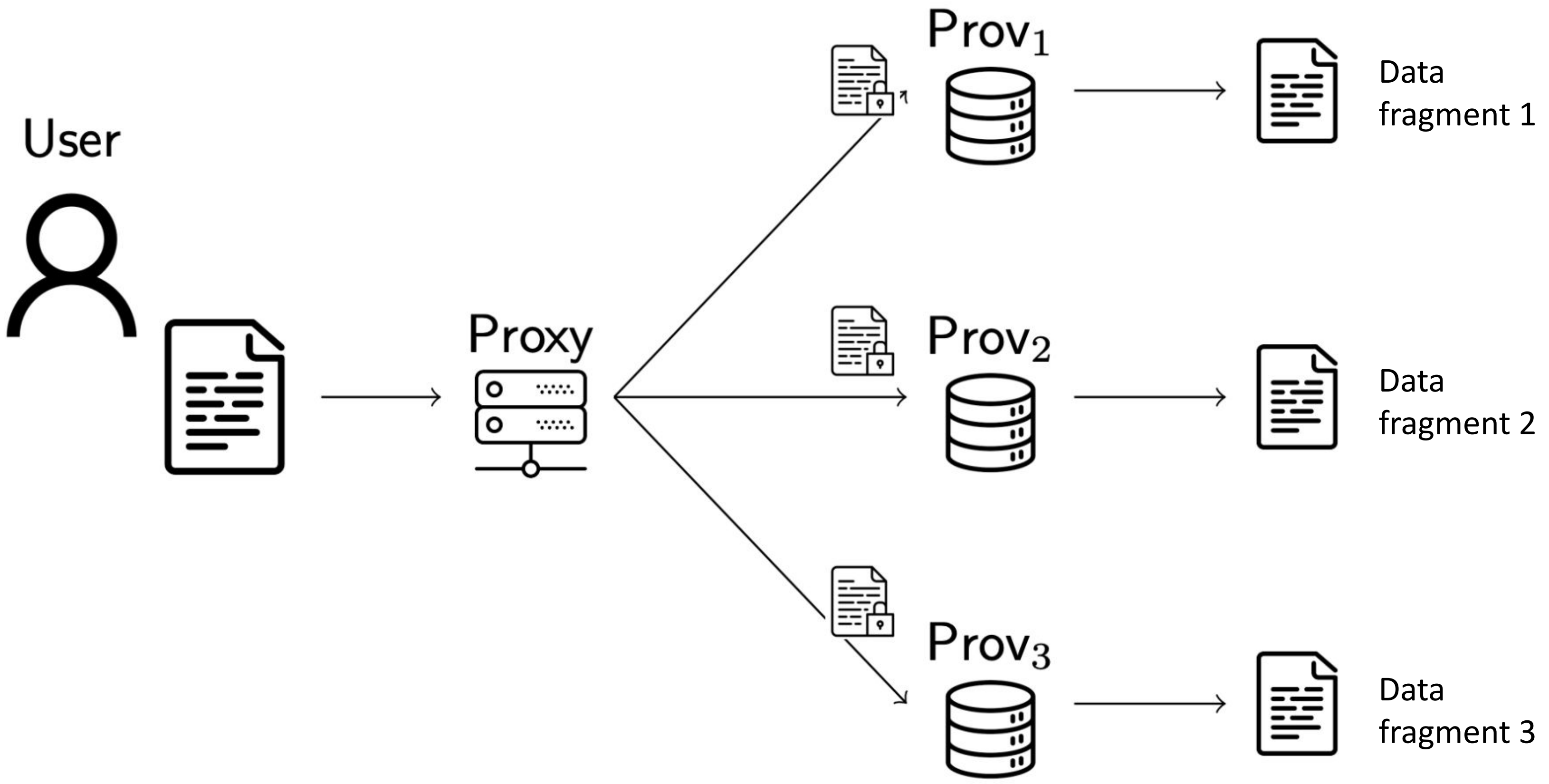
THRESHOLD CRYPTOGRAPHY

MULTI-PARTY STORAGE

ASTRAN S5

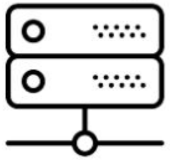
Secret
Shared
S3

Multi-cloud storage with a proxy



MPS and threshold modeling possibilities

Proxy



A single proxy

Prov $_i$

n storage providers

Frag

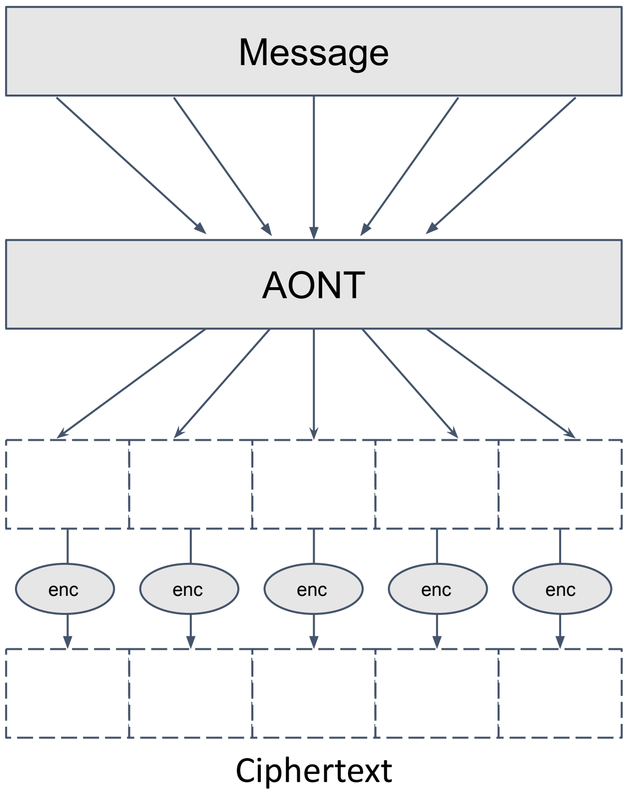
k out of n fragments threshold

n+1 adversaries → Independent dishonest attackers

n+1 adversaries → N-Collusion attacks < threshold

AONT

- All-Or-Nothing transform was introduced by Rivest[1] back in 1997.
- One must decrypt the entire ciphertext before one can determine even one message block.
- Original motivation: slowing down brute-force searches against all-or-nothing encryption blocks.

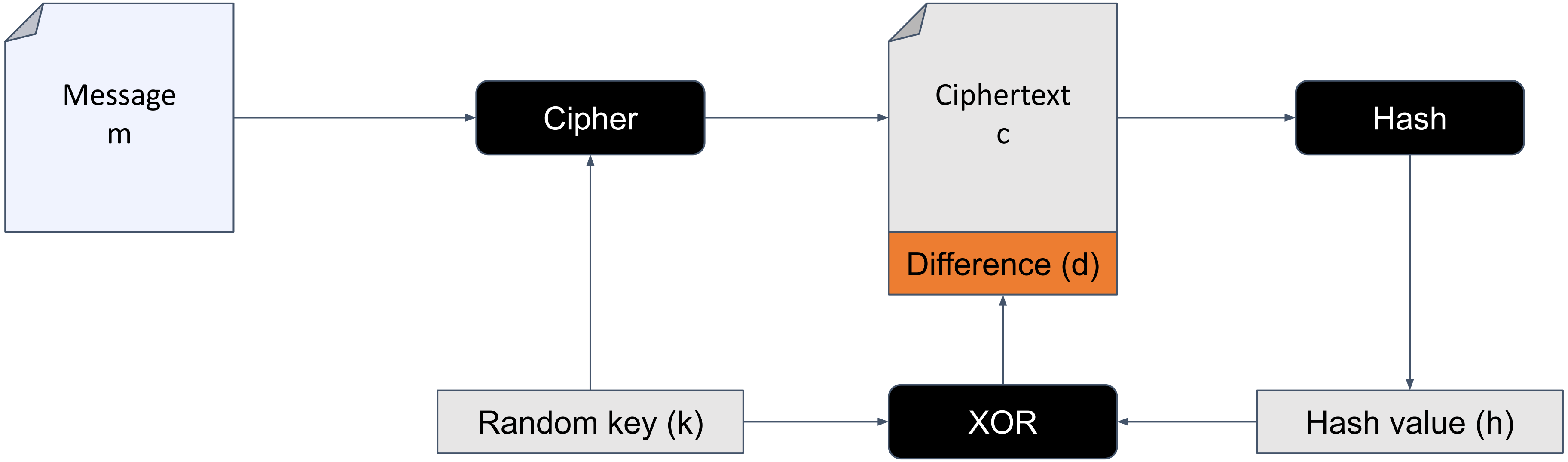


[1] R. L. Rivest. All-or-nothing encryption and the package transform. In E. Biham, editor, Fast Software Encryption, 4th International Workshop, FSE ’97, LNCS. Springer, 1997.

ALL OR NOTHING TRANSFORM IN PRACTICE

$$AONT(m) = Enc(m,k) \,||\, XOR(k,h)$$

where h = HASH(Enc(m,k))



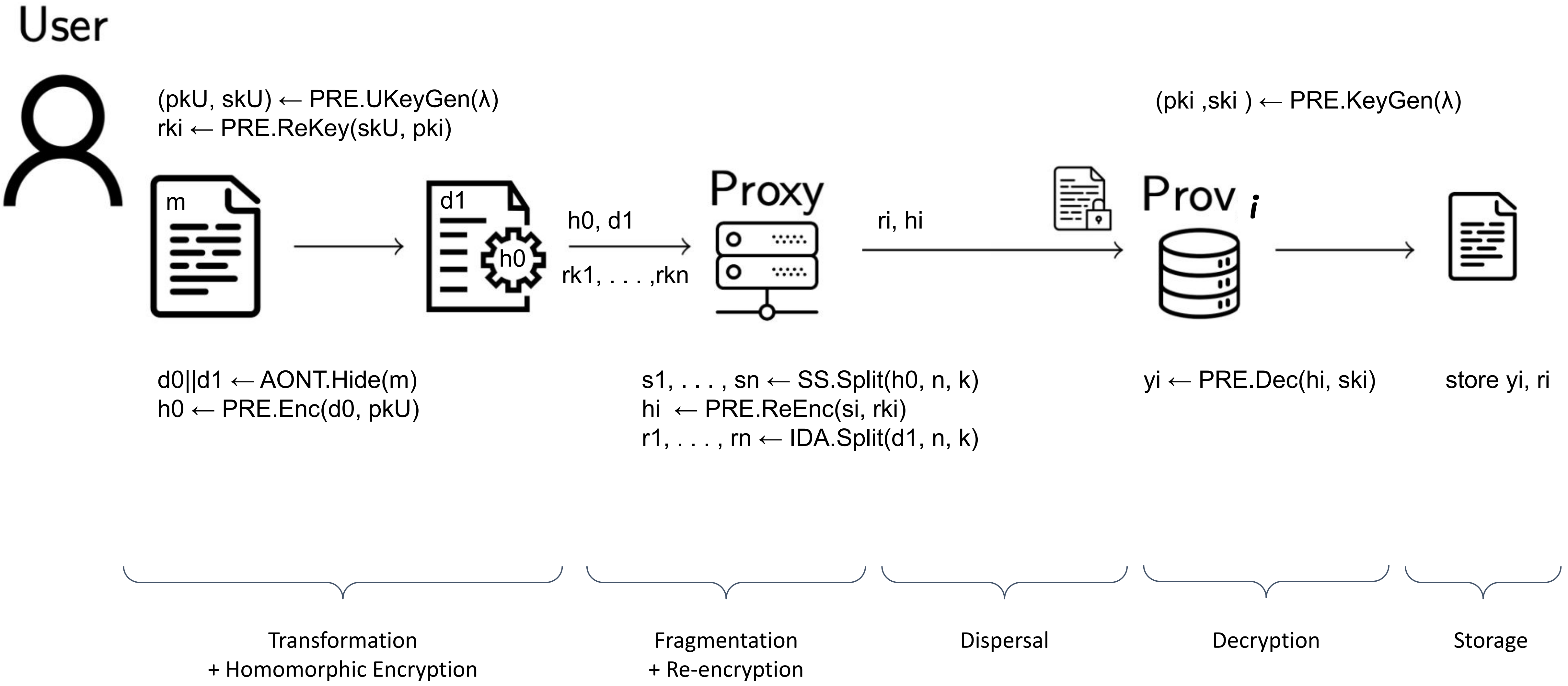
Can be used in conjunction with error coding, secret sharing, IDA or others threshold schemes

OTHER BUILDING BLOCKS

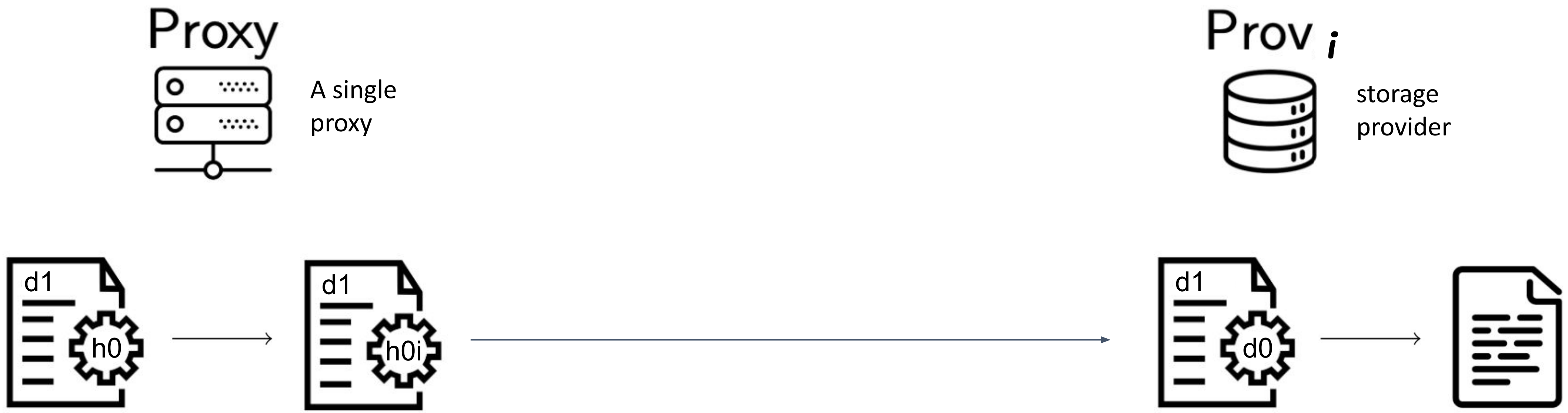
Secret Sharing Scheme (SSS)	We use Shamir's secret sharing [2]. It exploits the Lagrange interpolation theorem, specifically that k values suffice to uniquely determine a polynomial of degree ≤ k − 1. Shamir's secret sharing has perfect secrecy.
Information Dispersal Algorithm (IDA)	Unlike secret sharing, an IDA does not provide perfect-secrecy. However, an IDA is very memory-efficient. We are using algorithms similar to Rabin's IDA using erasure codes.
Proxy Re-Encryption Scheme (PRE)	We use in our protocols the fully homomorphic encryption scheme BGV [3]. Since BGV is fully homomorphic, it commutes with the secret sharing described above. It can perform proxy re-encryption by using the key-switching method described in [3].
Multikey Encryption Scheme (MKE)	We use multi-key homomorphic encryption [4] scheme. That way, the providers can also each decrypt their own share, this time with the participation of the others.

[2] A. Shamir. How to share a secret. Commun. ACM, 1979.
[3] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In S. Goldwasser, editor, Innovations in Theoretical Computer Science 2012. ACM, 2012
[4] A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. IACR Cryptol. ePrint Arch., 2013.

MPS USING HOMOMORPHIC PROXY RE-ENCRYPTION



2-collusion : dishonest proxy and provider



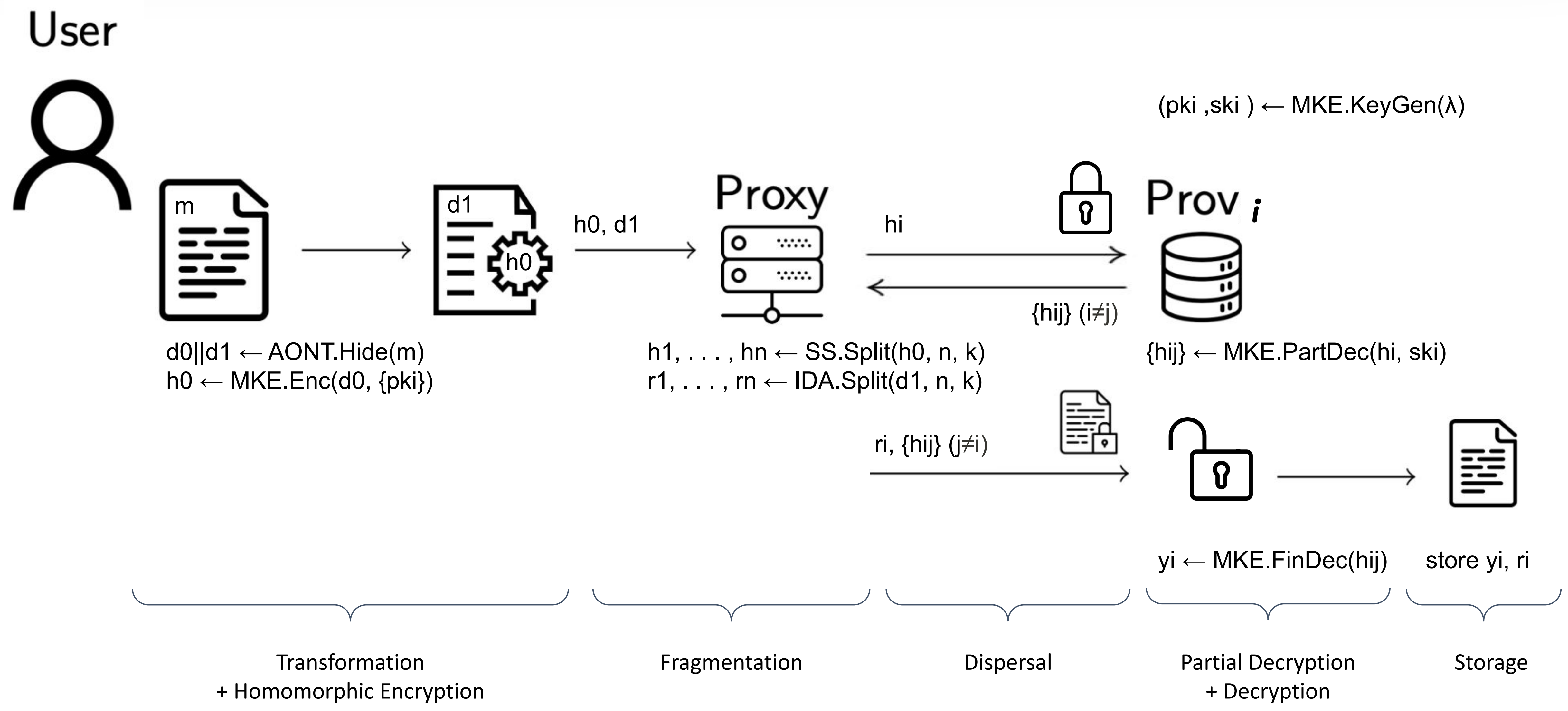
h0i ← PRE.ReEnc(h0, rki)

d0 ← PRE.Dec(h0i, ski)

m ← AONT.Reveal(d0||d1)

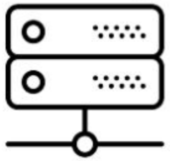
ASTRAN

MPS USING HOMOMORPHIC MULTIKEY ENCRYPTION



k-collusion :
dishonest proxy and k-1 providers

Proxy



A single proxy

$Prov_i$

n storage providers

Frag

k out of n fragments threshold

All-or-nothing Transform (AONT)

n out of n is a threshold!

Brings strong secrecy and integrity garanties

Memory-efficient for large volumes of data compared to SS

An essential building block in our current Multiparty Storage use case

A great and flexible gadget when combined with other schemes and algorithms

A generic scheme that can be implemented in many ways to provide additional threshold capabilities

Interested in our tech?

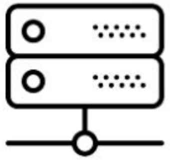
hello@astran.io

Ask Me (Almost) Anything

Appendices

THREAT MODELS

Proxy



A single proxy

Prov $_i$

n storage providers

Frag

k out of n fragments threshold

Provider-Secrecy	The data's confidentiality is preserved against cloud storage providers individually	The adversary plays the roles of a provider alone.
Proxy-Secrecy	The data's confidentiality is preserved against cloud proxy individually	The adversary plays the role of the proxy alone..
Provider-Collusion-Secrecy	The data's confidentiality is preserved against cloud storage providers collusion to a given threshold	The adversary plays the role of k colluding providers. k-provider-secrecy assumes the proxy is a trusted party.
Proxy-Provider-Collusion-Secrecy	The data's confidentiality is preserved against the proxy colluding with a given number of cloud storage provider	The adversary plays the role of the proxy and k colluding providers.