All Or Nothing Transform - Secret Sharing (AONT-SS)
A new secure multi-cloud storage scheme

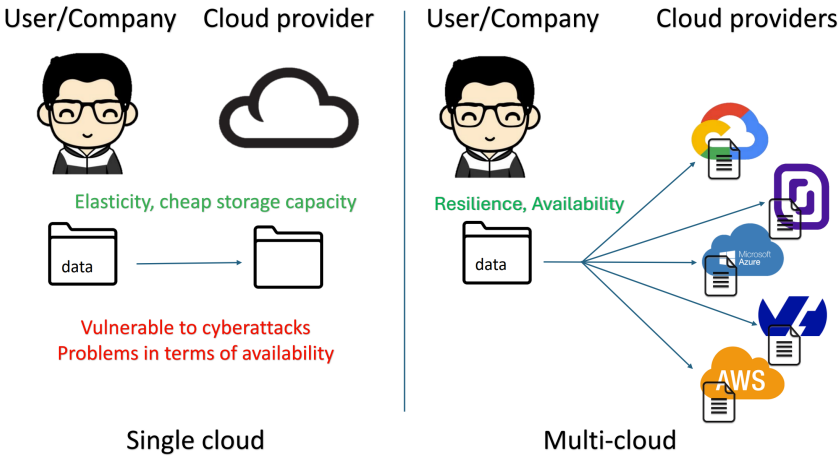
Dayane Horkos

Astran
EPITA

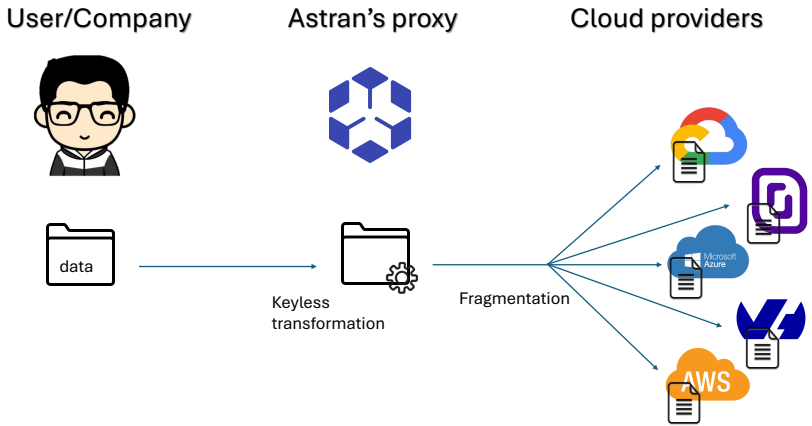
Supervised by: Gilles Seghaier (Astran), Prof. Ludovic Perret(LRE, EPITA)

April 2, 2025

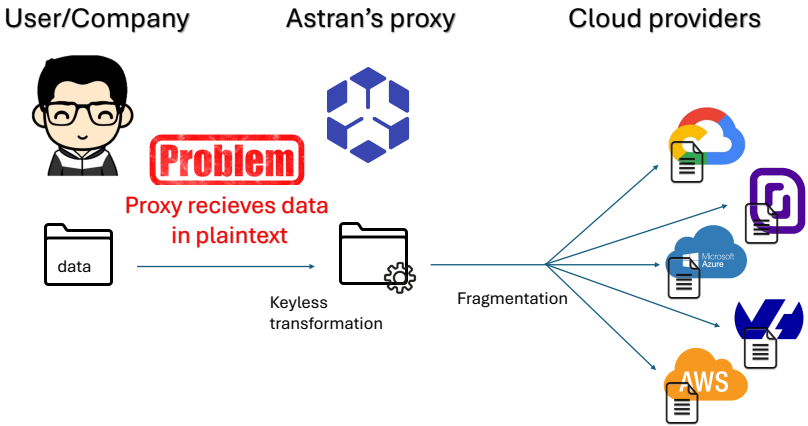
Clouds are everywhere



Presenting Astran and its usecase



Problem


User/Company
Astran's proxy
Cloud providers
Problem
Proxy recieves data
in plaintext
data
Keyless
transformation
Fragmentation
Microsoft
Azure
AWS

Contributions and State of art

Design a new **Multi-Cloud Storage scheme** with the following requirements:

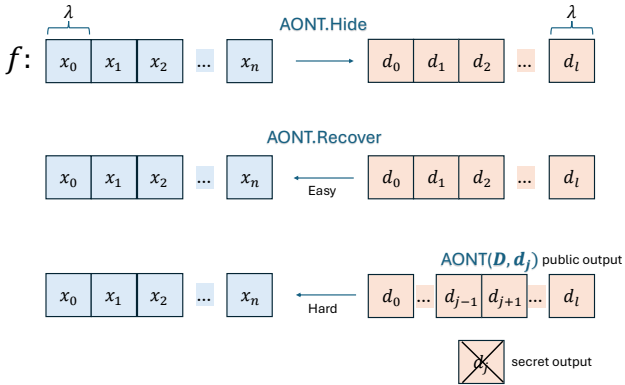
1. Goal: Achieve confidentiality against proxy
2. Constraint: Avoid complex management of encryption keys
3. Means: Requires some computations on the user's side

Examples of Multi-Cloud Storage schemes: [Resch and Plank, Usenix'11, Bessani et al., ACM'13, Zkik et al., IJCAC'17, Megouache et al., HCIS'20, Lafourcade et al., ESORICS'24]

AONT [Rivest, FSE'97]

Definition

An All-Or-Nothing Transform *AONT* [Rivest, FSE'97] is a transformation $f : \{0,1\}^* \to \{0,1\}^*$ such that



AONT-RP [Resch and Plank, Usenix'11, Chen et al., Africacrypt'2017]

The $AONT - RP$.Hide algorithm:

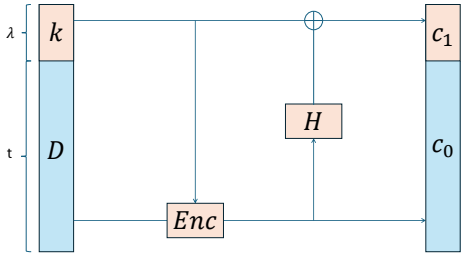
$k \leftarrow\$ \mathcal{K} = KeyGen(\lambda)$

$c_0 \leftarrow SKE.Enc_k(\mathcal{D})$

$c_1 \leftarrow k \oplus h(c_0)$

$c = AONT(\mathcal{D}) = c_0||c_1 = d_0||\dots||d_l$

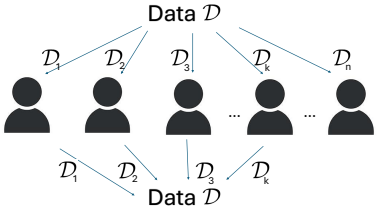
return c



PSS and IDA

Definition

Perfect Secret Sharing Scheme	**Information Dispersal Algorithm**
(k, n) threshold scheme	(k, n) threshold scheme
Provides **information theoretic security**	Sacrifices perfect security for **space efficiency**
Share size: $\|\mathcal{D}_i\| = \|\mathcal{D}\|$	Share size: $\|\mathcal{D}_i\| = \|\mathcal{D}\|/k$



New protocol **AONT-SS**:

1. Use an **AONT** to transform the data and dilute the key.
2. Create a tradeoff between security and space:
   - Use **PSS** on the secret output to provide confidentiality.
   - Use **IDA** on the public output to provide space efficiency.
3. Use a Certificate Authority to vouch for the public keys of each entity.

$AONT - SS$ Upload $(\mathcal{D}, index)$

User  **Proxy**  **Cloud Provider** i 

$d_0||\ldots||d_l \leftarrow AONT.Hide(\mathcal{D})$

$s_1, ..., s_n \leftarrow PSS.Share(d_j, n, k)$

$e_i \leftarrow PKE.E_{\mathsf{pk}_i}(s_i)$

$$\xrightarrow{AONT(\mathcal{D}, j), e_i}$$

$AONT - SS$ Upload $(\mathcal{D}, index)$

User  **Proxy**  **Cloud Provider** i 

$d_0||\ldots||d_l \leftarrow AONT.Hide(\mathcal{D})$

$s_1, ..., s_n \leftarrow PSS.Share(d_j, n, k)$

$e_i \leftarrow PKE.E_{\mathsf{pk}_i}(s_i)$

$AONT(\mathcal{D}, j), e_i \longrightarrow$

$r_i \leftarrow IDA.Disp(AONT(\mathcal{D}, j), n, k)$

$1 \leq i \leq n$

$r_i, e_i \longrightarrow$

$AONT - SS$ Upload $(\mathcal{D}, index)$

User	**Proxy**	**Cloud Provider** i
$d_0 \| \| \ldots \| \| d_l \leftarrow AONT.Hide(\mathcal{D})$		
$s_1, ..., s_n \leftarrow PSS.Share(d_j, n, k)$		
$e_i \leftarrow PKE.E_{\mathsf{pk}_i}(s_i)$		
$\xrightarrow{AONT(\mathcal{D}, j), e_i}$	$r_i \leftarrow IDA.Disp(AONT(\mathcal{D}, j), n, k)$	
	$1 \leq i \leq n$	
	$\xrightarrow{r_i, e_i}$	$s_i \leftarrow PKE.D_{\mathsf{sk}_i}(e_i)$
		store (r_i, s_i)

Proof of privacy

New theorem

*Assuming an honest-but-curious adversary $\mathcal{A}_{AONT-SS}$ representing the proxy and $k-1$ cloud providers, the scheme $AONT-SS$ has **IND security** when:*

- *PKE is IND-CPA*
- *PSS has perfect security*
- *$AONT$ has IND security*

Proof of privacy

New theorem

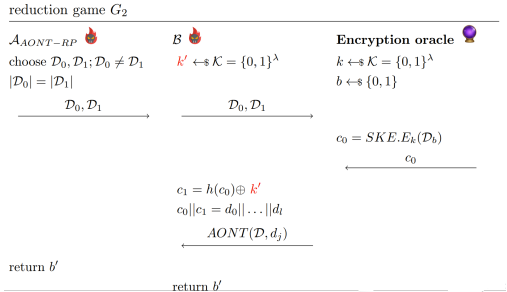
Assuming an honest-but-curious adversary $\mathcal{A}_{AONT-SS}$ representing the proxy and $k-1$ cloud providers, the scheme $AONT-SS$ has ***IND security*** *when:*

- *PKE is IND-CPA*
- *PSS has perfect security*
- *$AONT$ has IND security*

Proof sketch

It is sufficient to prove that $AONT-RP$ has IND security in the ROM when SKE is IND-CPA. Consider G_0 the game of IND-CPA of $\mathcal{SKE}$, G_1 the game of IND security of $AONT-RP$. The proof will proceed via game hopping and will consist of three steps.

1. We modify G_1 to get G_2, a new game with two keys, one for the encryption and one for the xor operation.
2. Reduction from game G_0 to G_2: $\Pr(\mathcal{B}$ wins $G_0)$=$\Pr(\mathcal{A}_{AONT-RP}$ wins in $G_2)$.



3. We compare the advantages of the adversaries in both games G_1 and G_2: $|Pr(\mathcal{A}_{AONT-RP}$ wins in $G_2) - Pr(\mathcal{A}_{AONT-RP}$ wins in $G_1)| < \epsilon$.

Conclusion

Results:

- We have presented a new multi-cloud scheme $AONT - SS$
- We extended $AONT - SS$ to another type of adversary: malicious with abort
- We also started studying how this scheme would be integrated into Astran

Future directions:

- Ongoing paper
- Thesis about Multi-Cloud Storage (MCS) schemes

Thank You for your attention!

Feel free to connect with me

LinkedIn: 

Email: dayane.horkos@astran.ai

Alysson Neves Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa. Depsky: Dependable and secure storage in a cloud-of-clouds. *ACM Trans. Storage*, 9(4):12, ACM'13. doi: 10.1145/2535929. URL `https://doi.org/10.1145/2535929`.

Liqun Chen, Thalia M. Laing, and Keith M. Martin. Revisiting and extending the AONT-RS scheme: A robust computationally secure secret sharing scheme. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Proceedings of the 8th International Conference on Cryptology in Africa (AFRICACRYPT 2017)*, volume 10239 of *Lecture Notes in Computer Science*, pages 40–57, Dakar, Senegal, May Africacrypt'2017. Springer. doi: 10.1007/978-3-319-57339-7_3.

Pascal Lafourcade, Lola-Baie Mallordy, Charles Olivier-Anclin, and Léo Robert. Secure keyless multi-party storage scheme. In Joaquín García-Alfaro, Rafal Kozik, Michal Choras, and Sokratis K. Katsikas, editors, *Computer Security - ESORICS 2024 - 29th European Symposium on Research in Computer Security, Bydgoszcz, Poland, September 16-20, 2024, Proceedings, Part III*, volume 14984 of *Lecture Notes in Computer Science*, pages 279–298. Springer, ESORICS'24. doi: 10.1007/978-3-031-70896-1_14. URL `https://doi.org/10.1007/978-3-031-70896-1_14`.

Leila Megouache, Abdelhafid Zitouni, and Mahieddine Djoudi. Ensuring user authentication and data integrity in multi-cloud environment. *Hum. centric Comput. Inf. Sci.*, 10:15, HCIS'20. doi: 10.1186/S13673-020-00224-Y. URL `https://doi.org/10.1186/s13673-020-00224-y`.

Jason K. Resch and James S. Plank. Aont-rs: Blending security and performance in dispersed storage systems. In Gregory R. Ganger and John Wilkes, editors, *9th USENIX Conference on File and Storage Technologies, San Jose, CA, USA, February 15-17, 2011*, pages 191–202. USENIX, Usenix'11. URL `http://www.usenix.org/events/fast11/tech/techAbstracts.html#Resch`.

Ronald L. Rivest. All-or-nothing encryption and the package transform. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 210–218. Springer, FSE'97. doi: 10.1007/BFb0052348. URL `https://doi.org/10.1007/BFb0052348`.

Karim Zkik, Ghizlane Orhanou, and Said El Hajji. Secure mobile multi cloud architecture for authentication and data storage. *Int. J. Cloud Appl. Comput.*, 7 (2):62–76, IJCAC'17. doi: 10.4018/IJCAC.2017040105. URL `https://doi.org/10.4018/IJCAC.2017040105`.