KU LEUVEN

Cross-Domain Attribute-Based Access Control Encryption (Possible Blockchain Applications)

Mahdi Sedaghat [1], Bart Preneel

imec-COSIC, KU Leuven, Belgium

2021/074

ssedagha@esat.kuleuven.be
22/07/2021

Outline:

Cross-Domain Attribute-Based Access Control Encryption scheme (CD-ABACE)

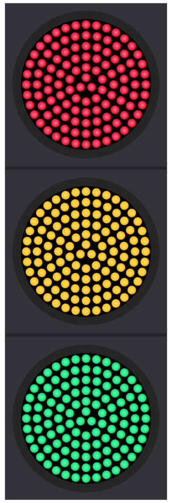
- Main applications and use cases
- Model
- Challenges and security requirements
- Main Ingredients
  - Structure-Preserving Signatures
  - Non-interactive Zero-Knowledge proofs
  - (Re-randomizable) Ciphertext-Policy Attribute-Based Encryptions
- Wrapping up
- Performance Analysis
- An application in Privacy-Balancing Blockchains
- Open problems
- References

Presentation light

Complicated but for those who are interested

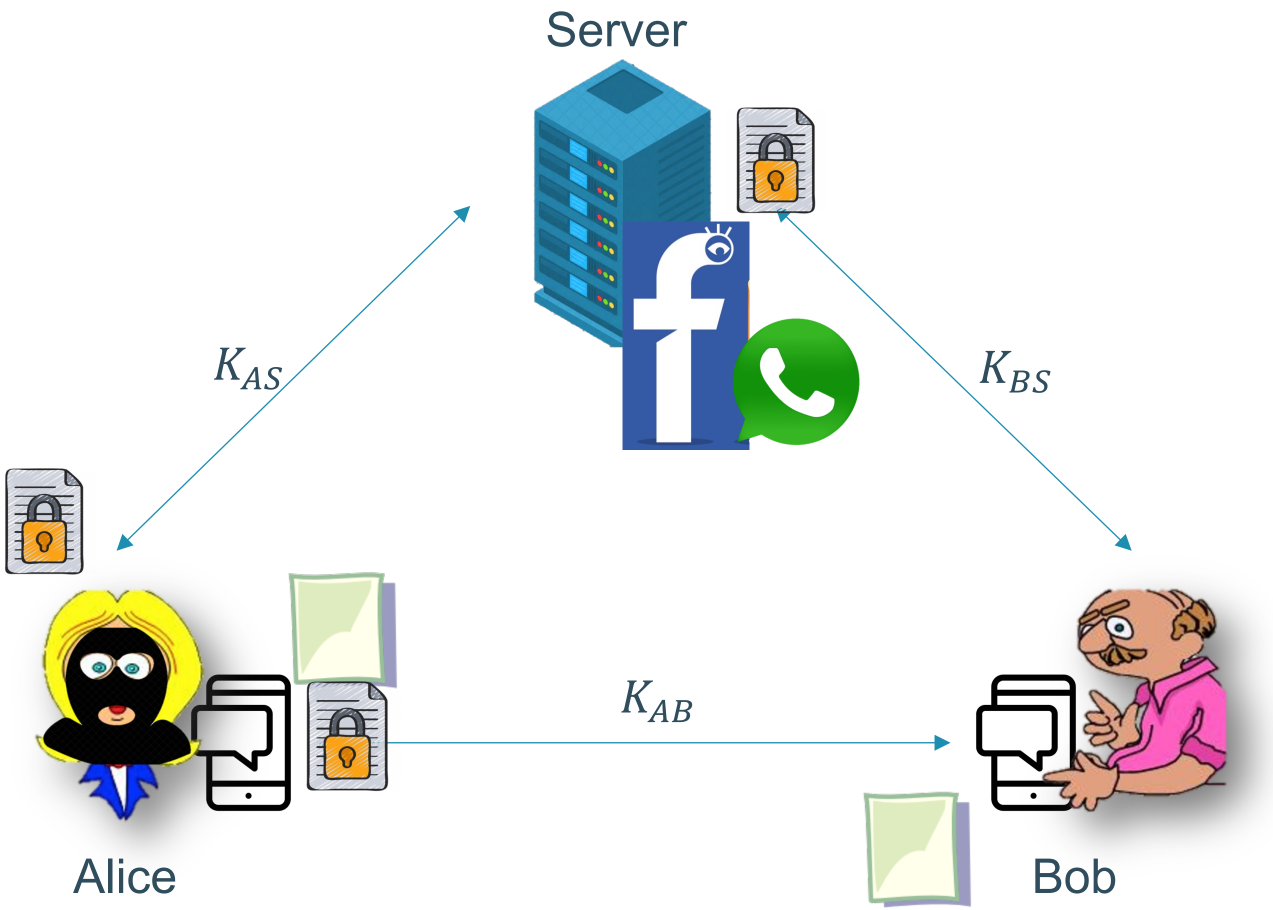
Fundamental and a bit hard to follow

Fundamental and easy to follow



Problem Statement:

Broadcasting malicious files
Criminal using
Terrorist activities

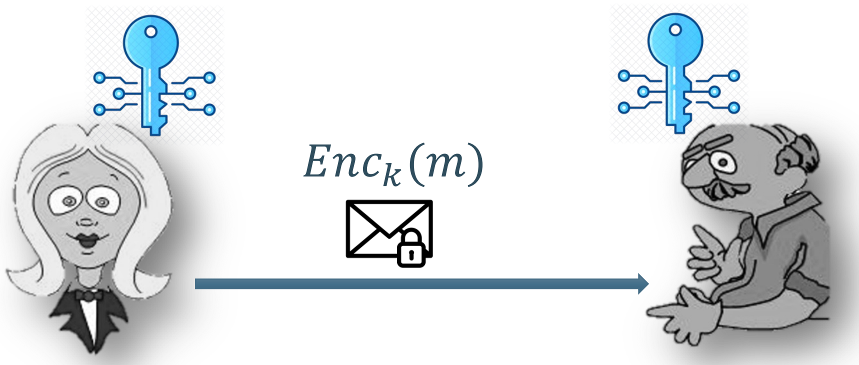


Key management
Big point of failure
Users' privacy

Access Control Encryption [DHO16]:

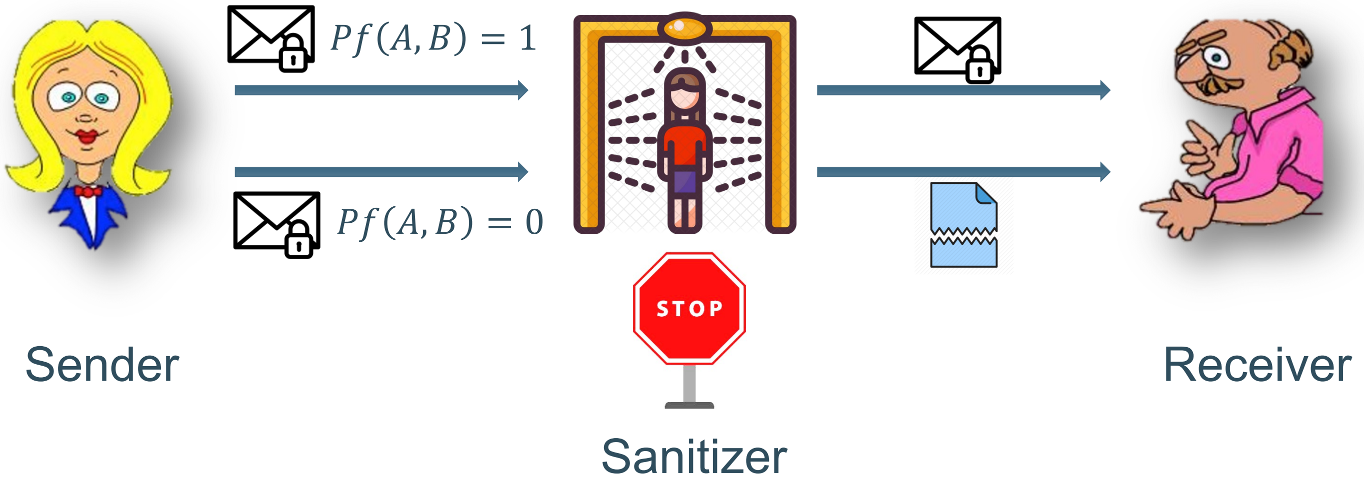
Only authorized users can communicate based on a fixed predicate function

In traditional Cryptography:
Everyone can read a ciphertext



The file might be malicious
The file might be a spam

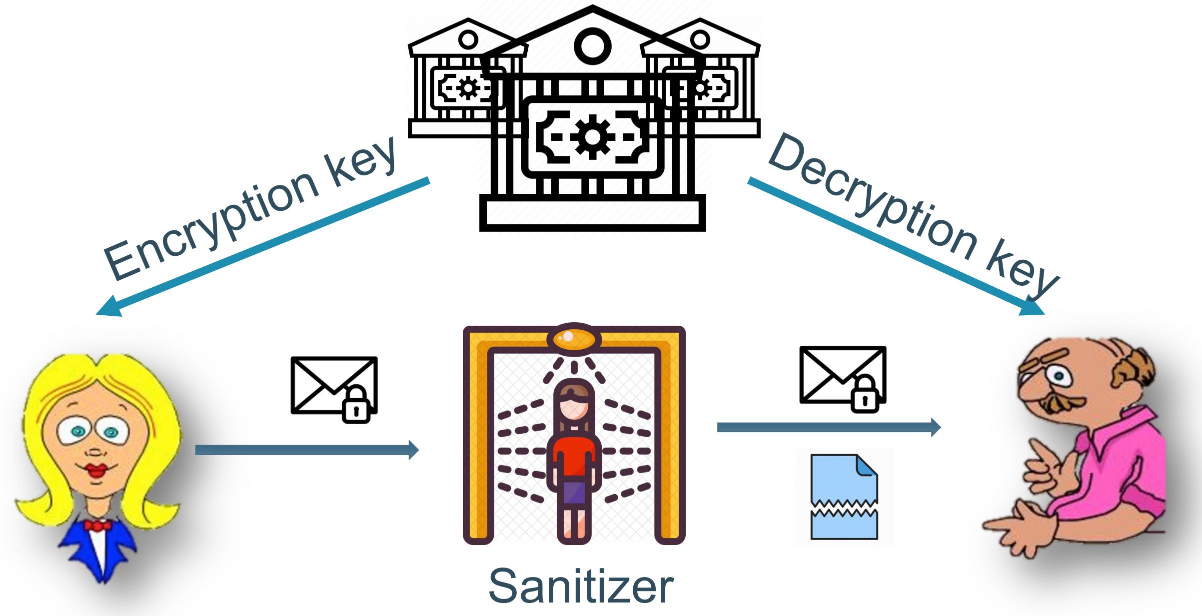
Fixed predicate function
$Pf(.)\colon \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$



Challenges:

ACE [Damgard et al, TCC 2016]

Cross-Domain ACE, [Wang and Chow, IEEE S&P 2021]



Fixed predicate function

$Pf(.)\colon \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

Security Requirements:
- No-Read rule
- No-Write rule

The Sanitizer is curious to learn
- Secret data
- Identity of the users

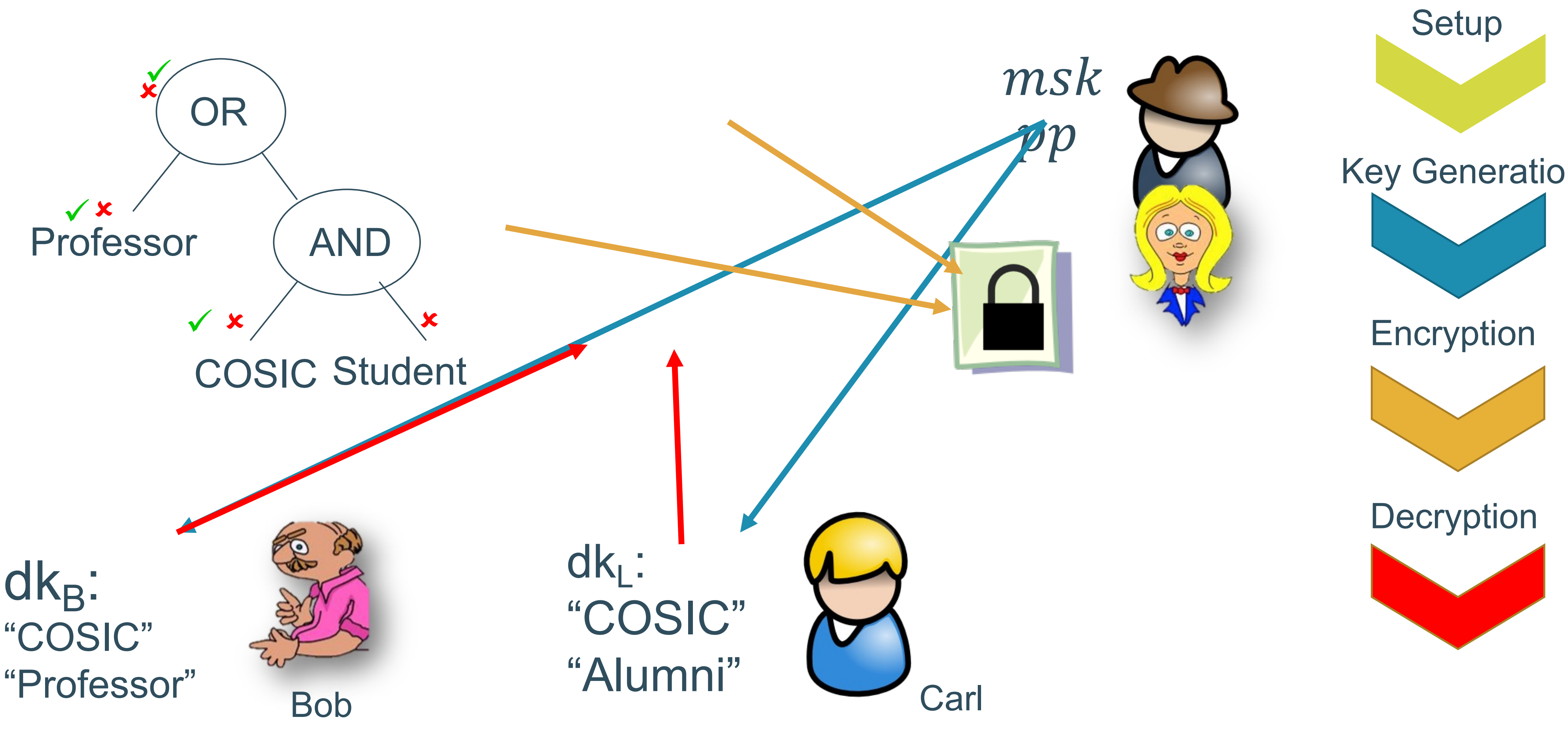
Extend it to Attribute-Based Predicate function
- Constant key size
- Constant ciphertext size

Our contributions:

n: the number of receivers and the total number of attributes in the system.
$r \ll n$: the maximum number of receivers that any sender is allowed to communicate with.
$s \ll n$: the maximum number of senders that any receiver can receive a message from.
$t \ll n$: the maximum number of attributes in any access policy that a sender can transmit data.
$w \ll n$: maximum number of legitimate attributes that any recipients possesses to decrypt a ciphertext

Scheme	Ciph. size	Enc. key size	Dec. key size	San. key size	Enc. size	Dec. cost	CD	PF	Assump.
[14, ‡ 3]	$O(2^n)$	$O(r)$	$O(1)$	$O(1)$	$O(n)$	$O(n)$	✓	IB	DDH/DCR
[14, ‡ 4]	$poly(n)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	✗	IB	iO
[18]	$O(n)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	✗	IB	SXDH
[26]	$poly(n)$	$O(1)$	$O(1)$	$O(1)$	$O(n)$	$O(n)$	✗	IB	DDH/LWE
[38] (SS)	$O(1)$	$O(1)$	$O(s)$	0	$O(1)$	$O(s)$	✓	IB	GBDP
Ours (SS)	$O(1)$	$O(1)$	$O(1)$	0	$O(1)$	$O(w)$	✓	AB	MSE-DDH

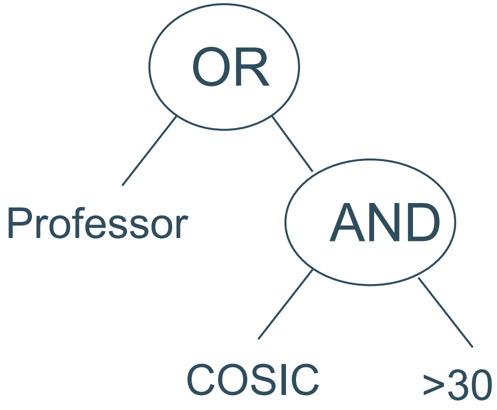
Ciphertext-Policy Attribute-Based Encryption [BSW07]



Attribute-Based Versus Identity-Based approaches:

	Bart	Akash	Aysajan	Roozbeh
Bart				
Akash	✓			
Aysajan	✓	✓		
Roozbeh	REJECT	✓	REJECT	

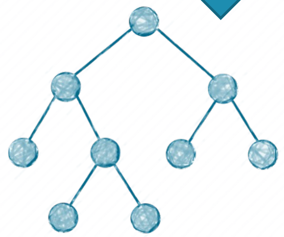
Identity-Based Predicate Function



dk:
"Cosic"
"Professor"
"Age>50"

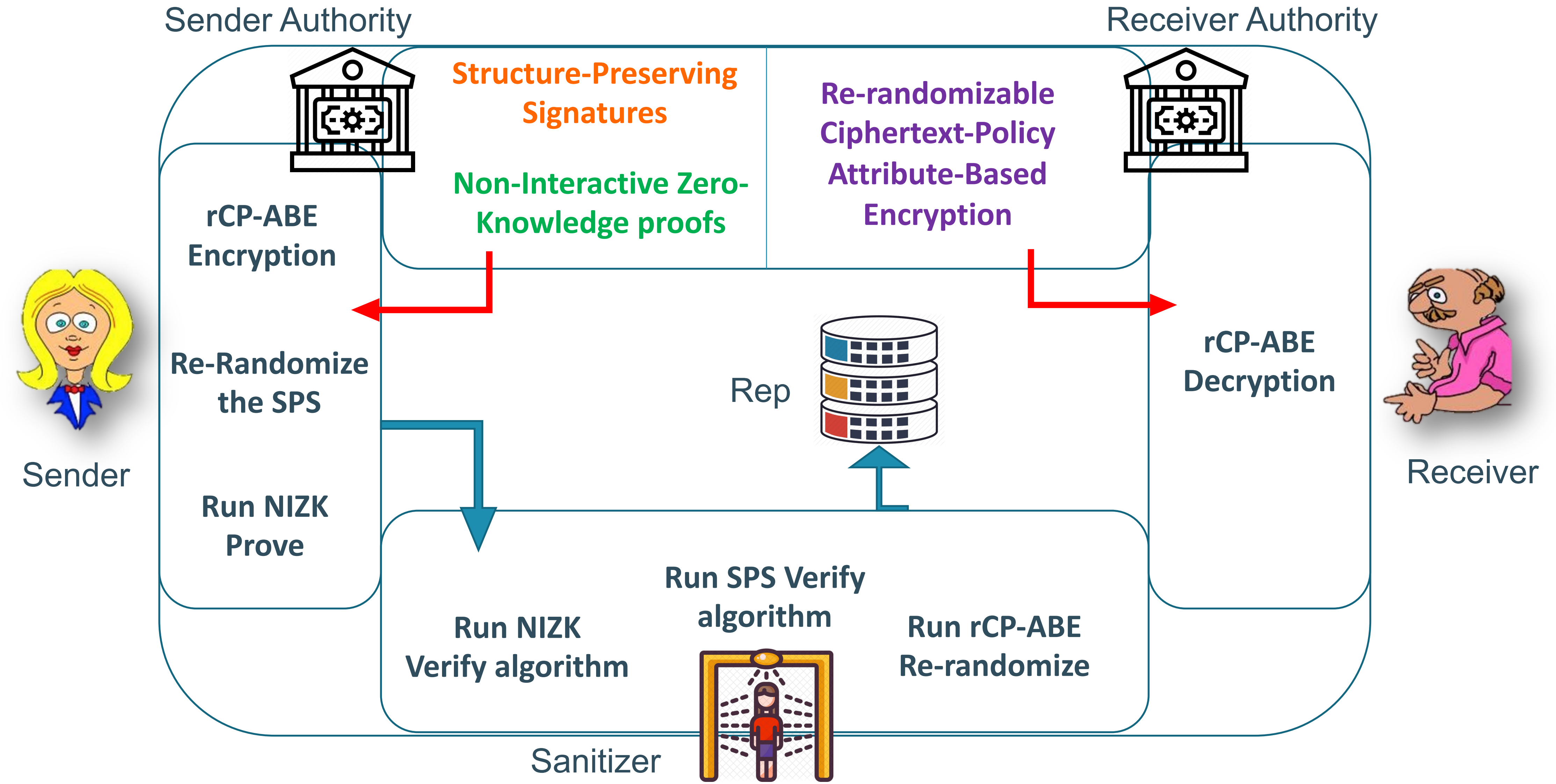
dk:
"Cosic"
"PhD"
"Age<30"

	Bart	Akash	Aysajan	Roozbeh
Bart				
Akash	✓			
Roozbeh	✓	✓		
Aysajan	REJECT	✓		REJECT



Attribute-Based Predicate Function

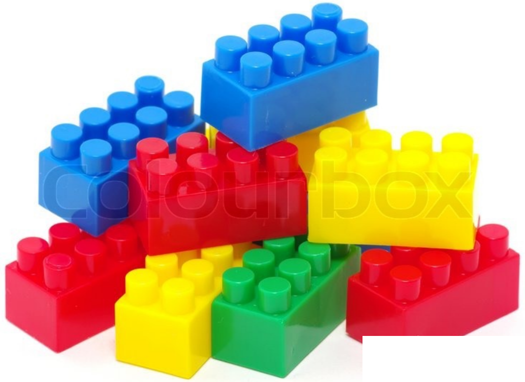
Generic Construction (main ingredients):



Structure-Preserving Signature (SPS) [Abe et al. 10]:

Mathematical Structures in Cryptography:
- ElGamal encryption
- Pedersen commitments
- Schnorr proofs

Pairing-based Cryptography:
- Identity-based encryption
- Short digital signatures
- NIZK proofs



Preserve Mathematical Structures in Pairing groups:
- Communication consists of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$
- Use generic group operations
  - Multiplication, membership testing, pairing
- Avoid structure-destroying operations
  - No cryptographical Hash functions

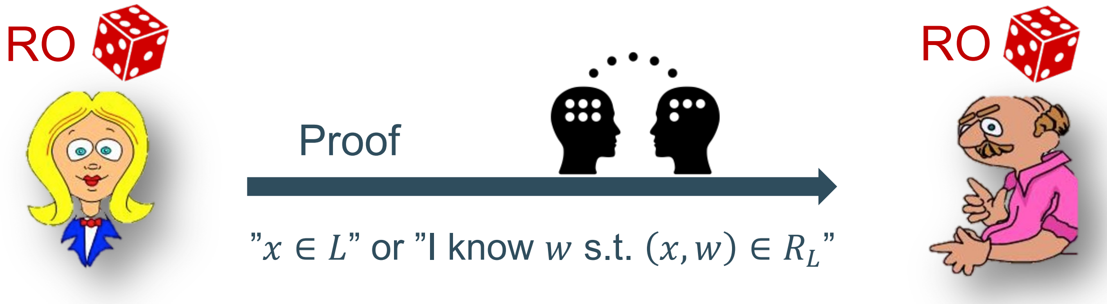
Modular Design
Makes easy to combine

ZK proofs:

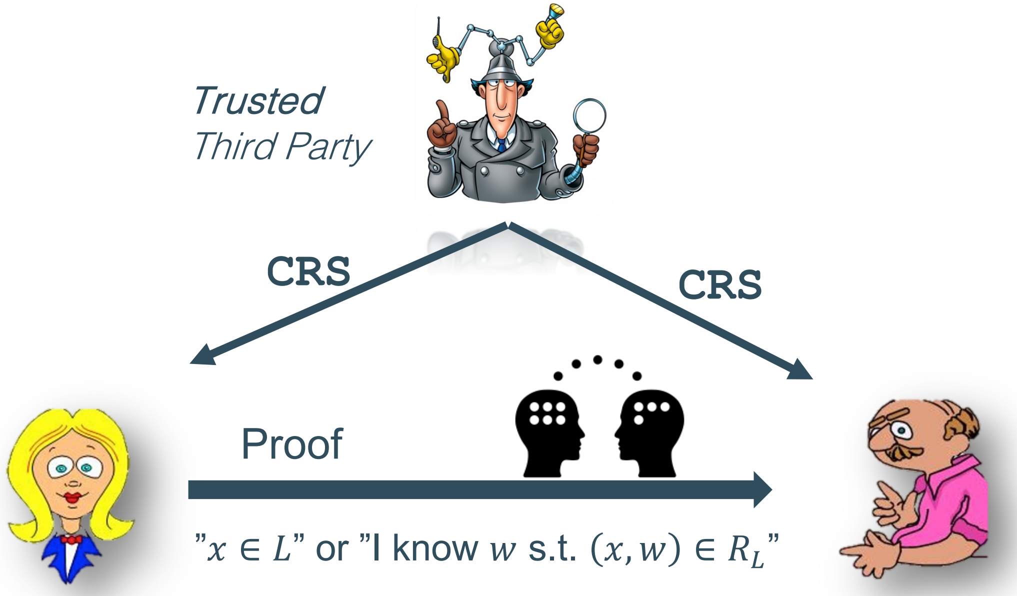
Non-Interactive Zero-Knowledge (NIZK) proof systems [GMR85]

- Non-Interactive zero-knowledge protocols are constructed in two models

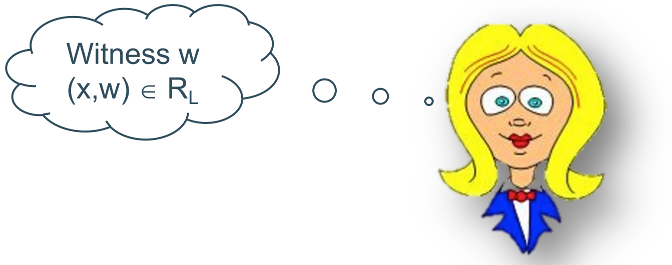
  - Random Oracle (RO) Model
    - Parties have access to an RO



  - Common Reference String (CRS) Model
    - Trusted Third Party generates a CRS



NIZKs: Security requirements

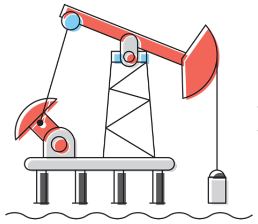


(stat, proof) ⟹

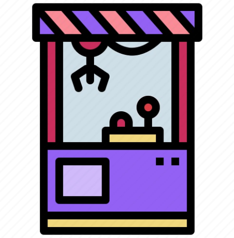
proof ←**Prove**(CRS, stat, witness)

{1, 0} ←**Verify**(CRS, stat, proof)

- **Completeness:** honest P always will convince the honest V
- **Zero-Knowledge (ZK):** dishonest V only gets to know that the statement is true.
- **Knowledge Soundness:** dishonest P cannot convince honest V, unless she knows some secret "wit"



`Ext`(proof, Ext-TD) → witness: (stat, witness) $\in R_L$

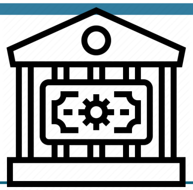


`Sim`(stat, Sim-TD) → proof' $\approx_c$ proof

The proposed rCP-ABE scheme:

Over the attribute space $\mathbb{U}$ of size n

Setup



Key Generation

$\alpha \leftarrow \mathbb{Z}_p^*$

$h_i = \{[\alpha^i]_2\}_{i\in[n]}$

$g_2 = [\alpha^2]_1$

$pp = \{h_i, g_2, [\alpha]_T\}$

$msk = \{\alpha, g\}$

Parse msk

$\mathbb{B} \subset \mathbb{U}$

$Z_{\mathbb{B}}(x) = \prod_{i=1} (x - k_i)^{1-b_i}$

$dk_{\mathbb{B}} = \left[\frac{1}{Z_{\mathbb{B}}(\alpha)}\right]_1$

Encryption

Parse pp

Defines $\mathbb{P} \subset \mathbb{U}$

$r \leftarrow \mathbb{Z}_p^*$

$Z_{\mathbb{P}}(x) = \prod_{i=1} (x - k_i)^{1-p_i}$

$C_1 = [r\alpha Z_{\mathbb{B}}(\alpha)]_2$

$C = m[r\alpha]_T$

$C_2 = g_2^{-r}$

$CT = (\mathbb{P}, C, C_1, C_2)$

CT →

$s \leftarrow \mathbb{Z}_p^*$

$Z_{\mathbb{P}}(x) = \prod_{i=1} (x - k_i)^{1-p_i}$

$\widetilde{C_1} = C_1 \times [s\alpha Z_{\mathbb{B}}(\alpha)]_2$

$\tilde{C} = C \times [s\alpha]_T$

$\widetilde{C_2} = g_2^{-r} \times g_2^{-s}$

$\widetilde{CT} = (\mathbb{P}, \tilde{C}, \widetilde{C_1}, \widetilde{C_2})$

Re-Randomizable

Parse pp and $dk_{\mathbb{B}}$

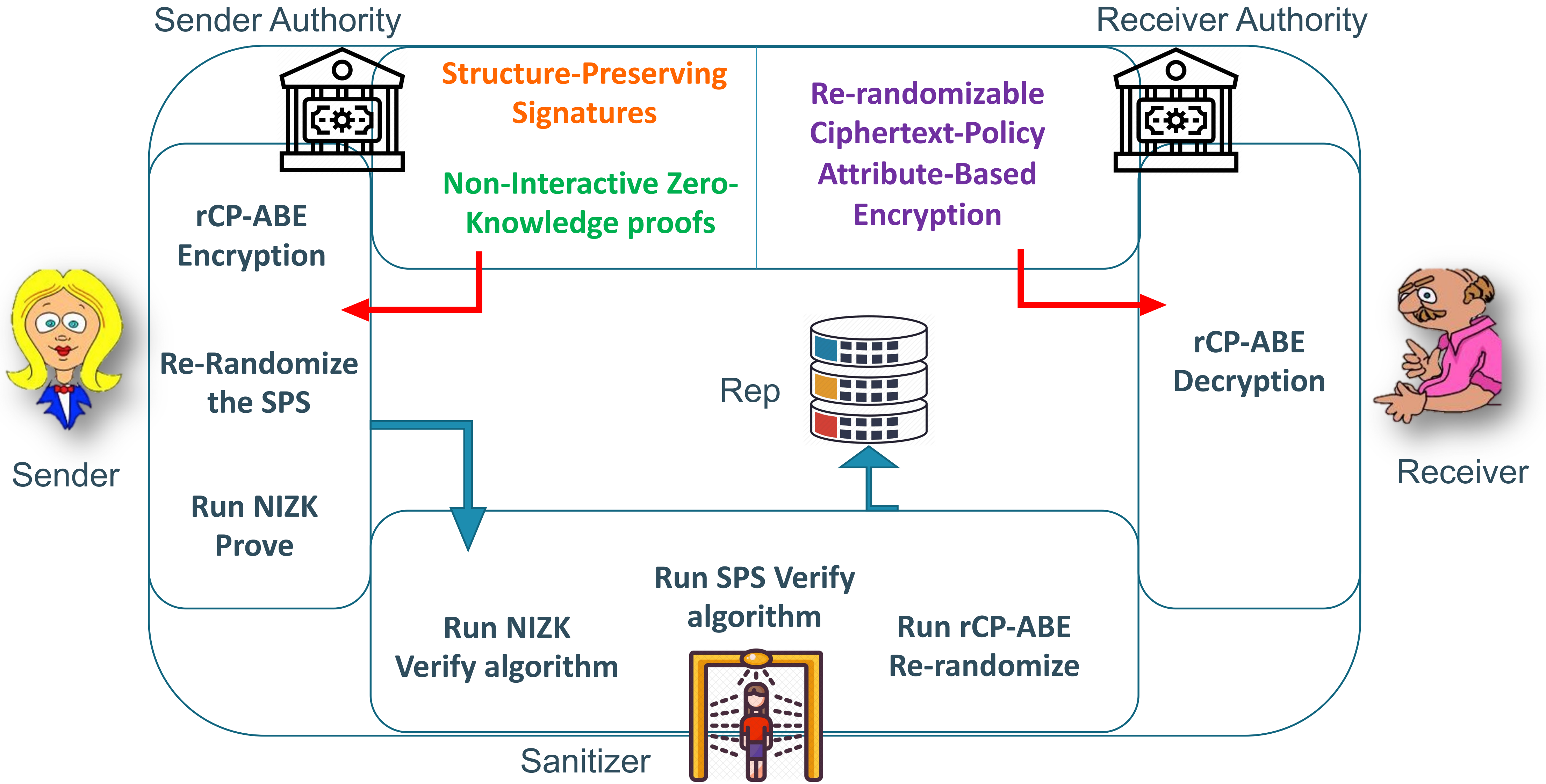
If $\mathbb{P} \subseteq \mathbb{B}$:

$c_i = b_i - p_i$

$F_{\mathbb{B},\mathbb{P}}(x) = \prod_{i=1} (x - k_i)^{c_i}$

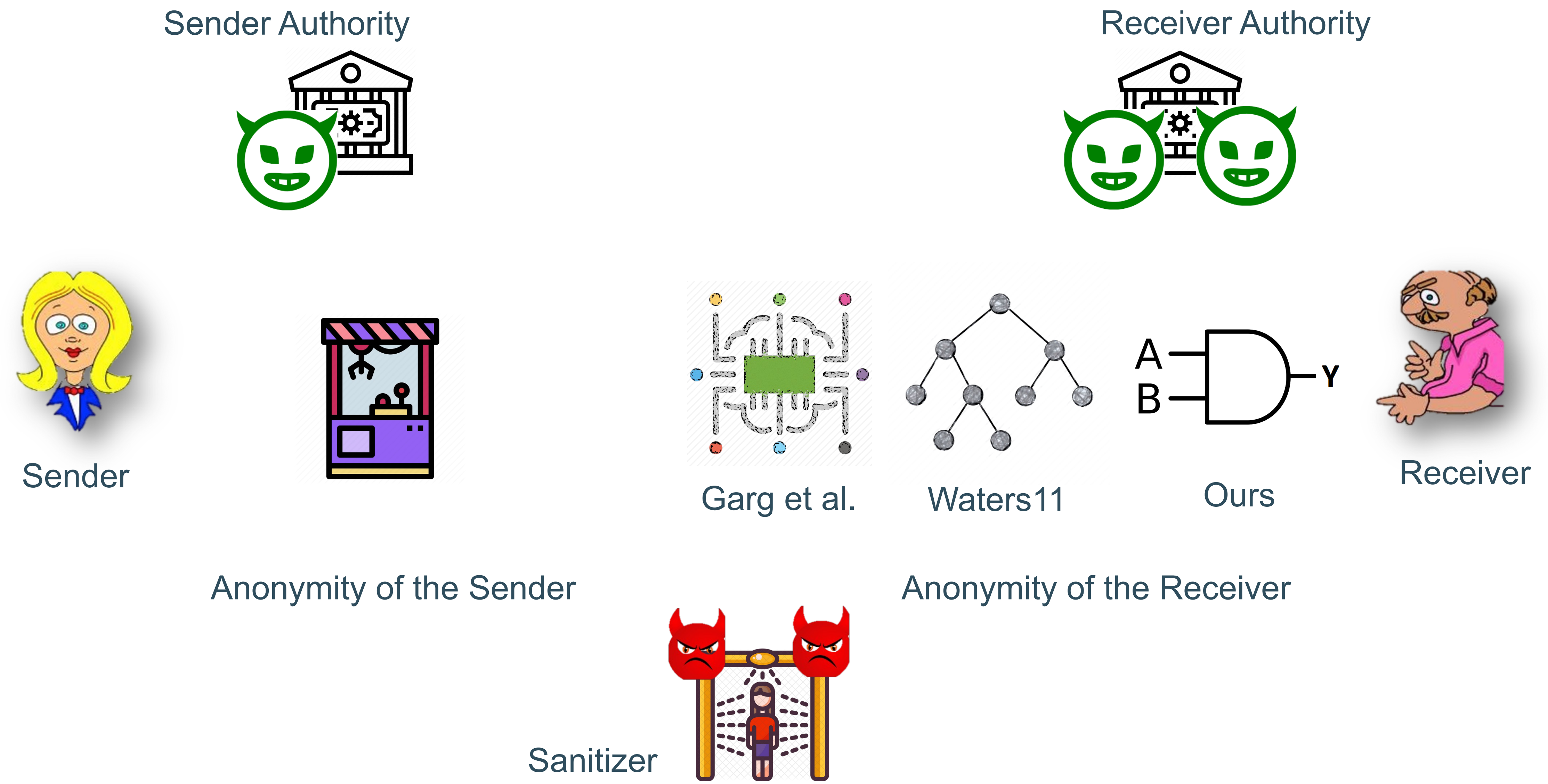
$m = C \times \left(e\left(C_2, \prod_{i=1}(h_{i-1})^{f_i}\right) \times e(dk_{\mathbb{B}}, C_1)\right)^{-1/f_0}$

Decryption



Sender Authority
Receiver Authority
Structure-Preserving Signatures
Non-Interactive Zero-Knowledge proofs
Re-randomizable Ciphertext-Policy Attribute-Based Encryption
rCP-ABE Encryption
Re-Randomize the SPS
Run NIZK Prove
Sender
Rep
rCP-ABE Decryption
Receiver
Run SPS Verify algorithm
Run NIZK Verify algorithm
Run rCP-ABE Re-randomize
Sanitizer

Tread Model and Users' Anonymity:



Implementation and open questions:

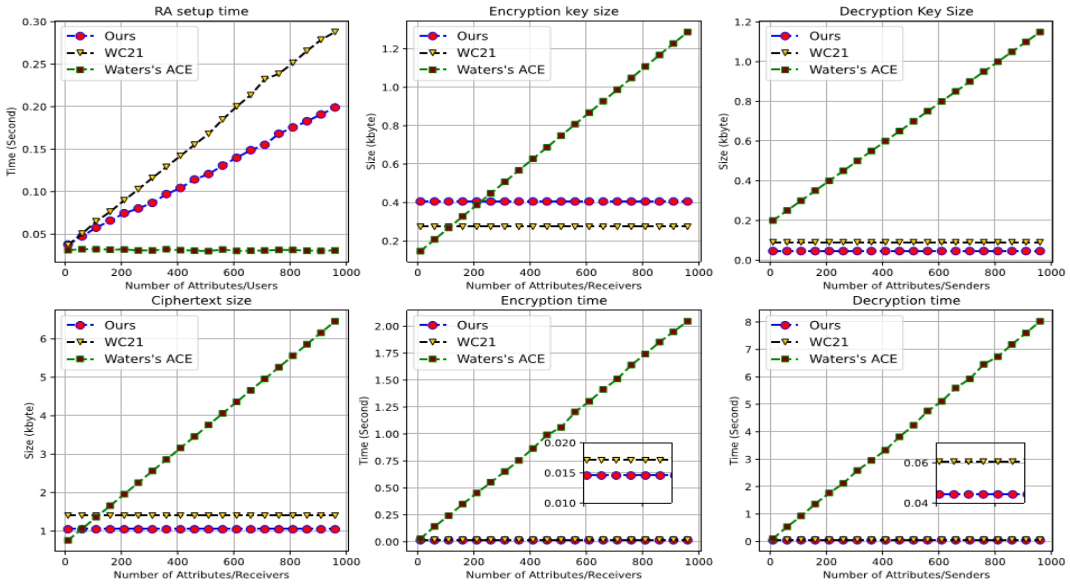
Open questions:

Improve the receiver anonymity with the same complexity.

More universal CP-ABE scheme with the same performance.

Achieving the same security requirements with different methods.

Decrease or eliminate the needed Sanitizer.



A Blockchain application for distributed AB-ACE

Blockchain — Decentralized and Immutable Ledger

Wasteful/ Throughput/ Latency/ Block size — **Bitcoin** — The privacy of the users is compromising.

Zcach [BCG14] as a cryptocurrency uses the ZK proofs — **Zero-Knowledge Proofs** — To address the privacy issue

Audit in the case of illicit activity — **Privacy-Balancing** — Ban those Tnxs that are not following some rules

Pseudonymity ≠ Anonymity

The PID of the **payee** and **payer** and the **value** in Bitcoin are publicly available

If Cosic pays employee in Bitcoin

All salaries are visible

Public Supply chain

Unlikable private payments

The identity and the values are hidden

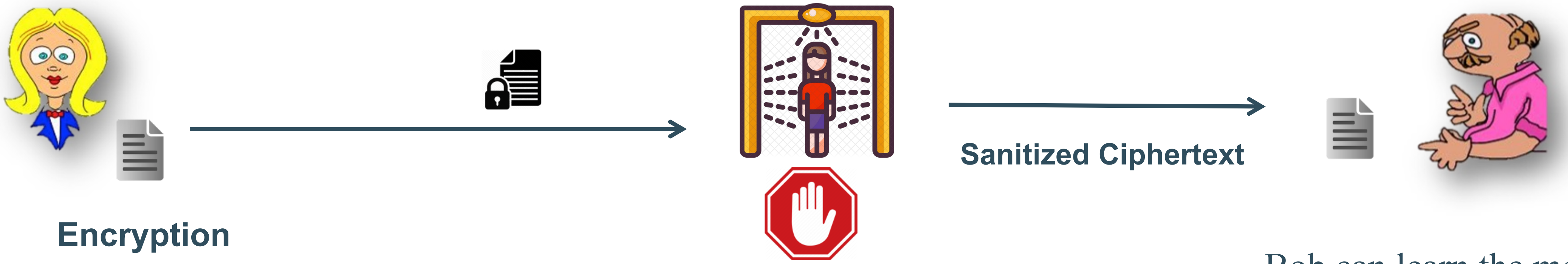
Such cryptocurrencies can be used in an illegal context

- Tax evasion
- Ransomware
- Drug trafficking
- Terrorist funding
- etc

Possible Solution:

Sender Authority

Receiver Authority



Predicate Function
$Pf(KYL, AML) \stackrel{?}{=} 1$

Bob can learn the message
iff $Pf(Alice, Bob) \stackrel{?}{=} 1$

References

[Abe10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Annual Cryptology Conference, pages 209–236. Springer, 2010.

[Abe14] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Theory of Cryptography Conference, pages 688–712. Springer, 2014.

[Bon04] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In International conference on the theory and applications of cryptographic techniques, pages 223–238. Springer, 2004.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07), pages 321–334. IEEE, 2007.

[Gro16] Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, EUROCRYPT 2016, Part II, volume 9666 of LNCS, pages 305–326. Springer, Heidelberg, May 2016.

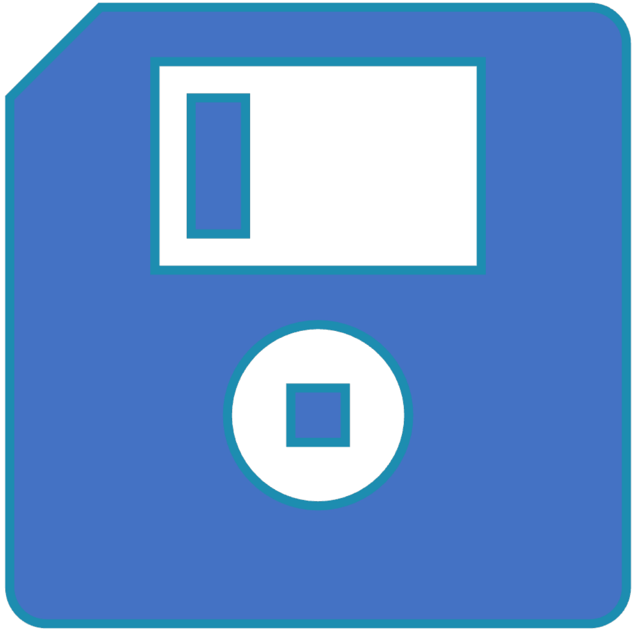
[DHO16] Ivan Damgård, Helene Haagh, and Claudio Orlandi. Access control encryption: Enforcing information flow with cryptography. In Theory of Cryptography Conference, pages 547–576. Springer, 2016.

[KW17] Sam Kim and David J Wu. Access control encryption for general policies from standard assumptions. In International Conference on the Theory and Application of Cryptology and Information Security, pages 471–501. Springer, 2017.

[WC21] Xiuhua Wang and Sherman S. M. Chow. Cross-domain access control encryption: Arbitrary-policy, constant-size, efficient. IEEE Symposium on Security and Privacy (S&P), 2021.

Thank You!

ssedagha@esat.kuleuven.be



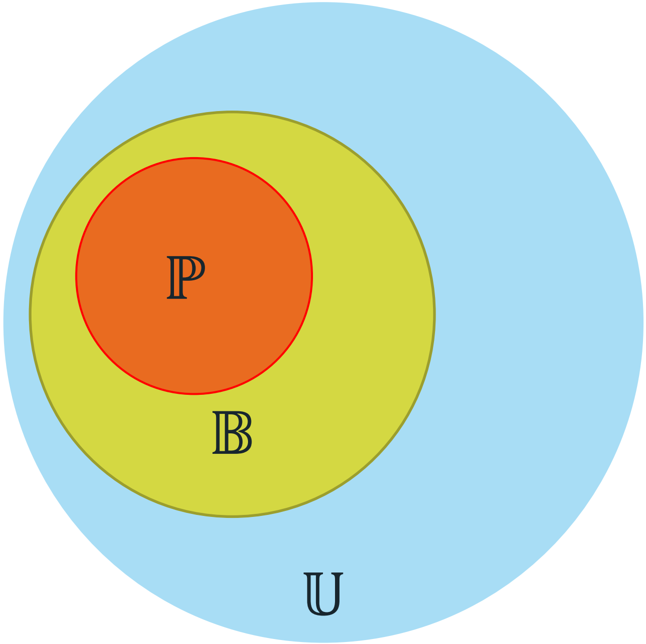
Backup slides

Definitions

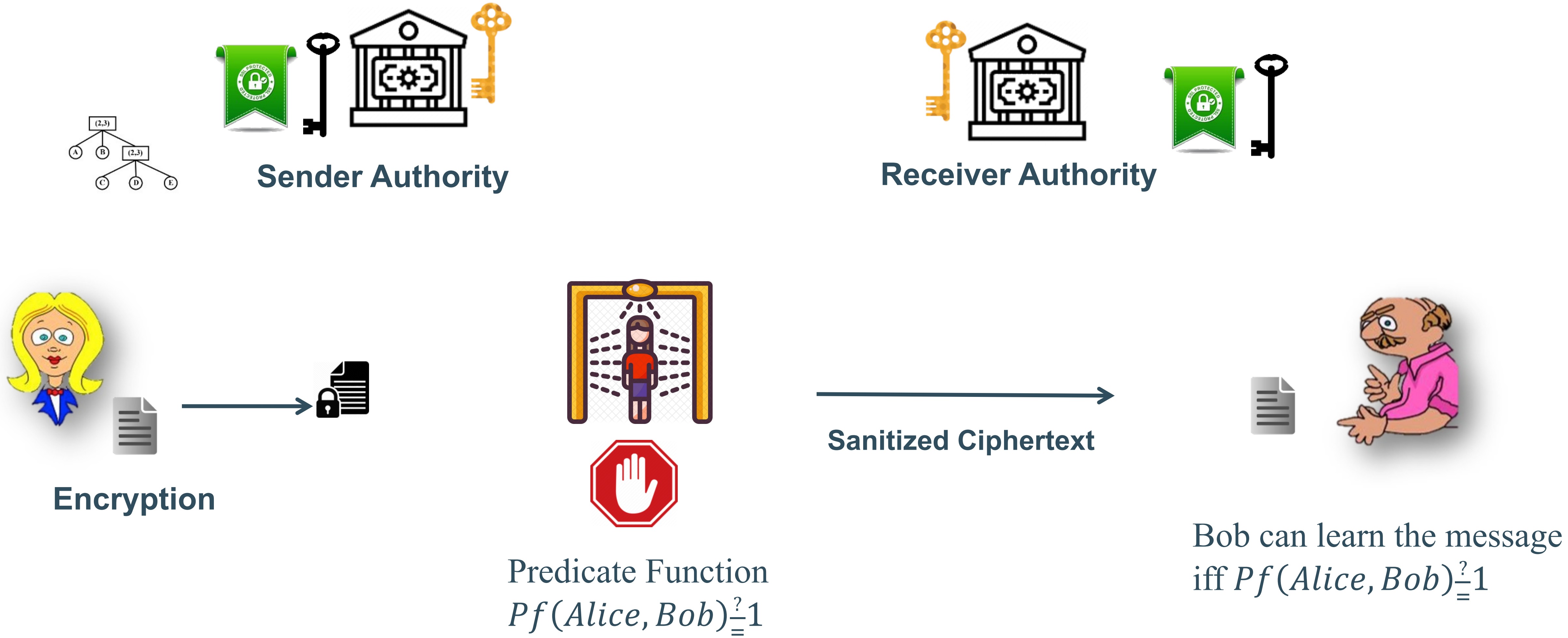
Bilinear Group setting:

Type-III: $\mathbb{G}_1 \neq \mathbb{G}_2$ and no homomorphism

- $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, \hat{e}, g, h) \leftarrow BGen(1^\lambda)$
  - Groups are cyclic of prime order p.
  - There exists an efficient map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$:
    - $\hat{e}(g^x, h^y) = \hat{e}(g, h)^{xy}$
    - $\mathbb{G}_1 =< g >, \mathbb{G}_2 =< h >, \mathbb{G}_T =< \hat{e}(g, h) >$



Attribute-Based Cross-Domain ACE

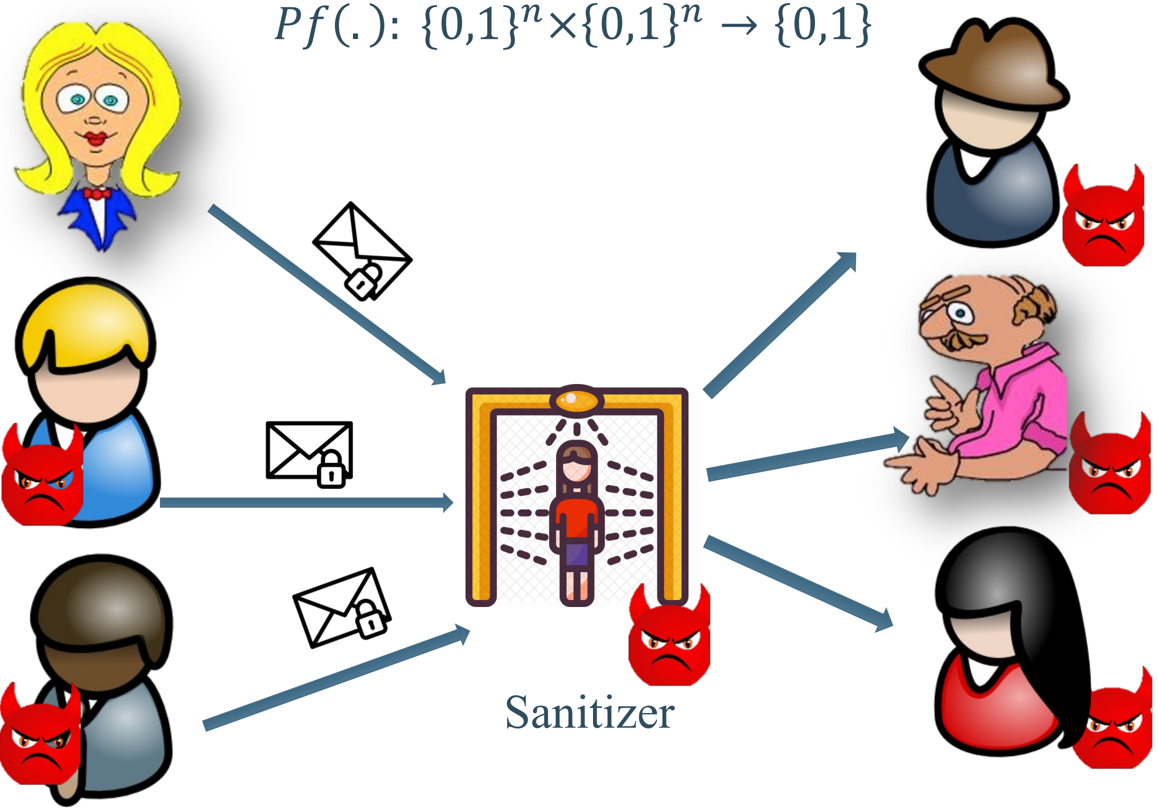


Security requirements:

No-Read rule

Fixed predicate function

$Pf(.)\colon \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$



Senders

Receivers

No-Read rule:

No malicious party without a valid decryption key can learn the secret message

$\textsc{No-Read}^{\mathcal{A}}_{\text{CD-ABACE}}(1^\lambda, \mathbb{U})$

1 : $(\mathsf{pp}_{ra}, \mathsf{msk}_{ra}) \leftarrow \mathsf{RAgen}(1^\lambda, \mathbb{U})$

2 : $(\mathsf{pp}_{sa}, \mathsf{msk}_{sa}) \leftarrow \mathsf{SAgen}(\mathsf{pp}_{ra}, \mathbf{R_L})$

3 : $\mathbb{P}^* \leftarrow \mathcal{A}(\mathsf{pp}_{ra}, \mathsf{pp}_{sa})$

4 : $(m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pp}_{ra}, \mathsf{pp}_{sa})$

5 : $(\mathsf{ek}_{\mathbb{P}^*}, \sigma^*, W^*) \leftarrow \mathsf{EncKGen}(\mathbb{P}^*)$

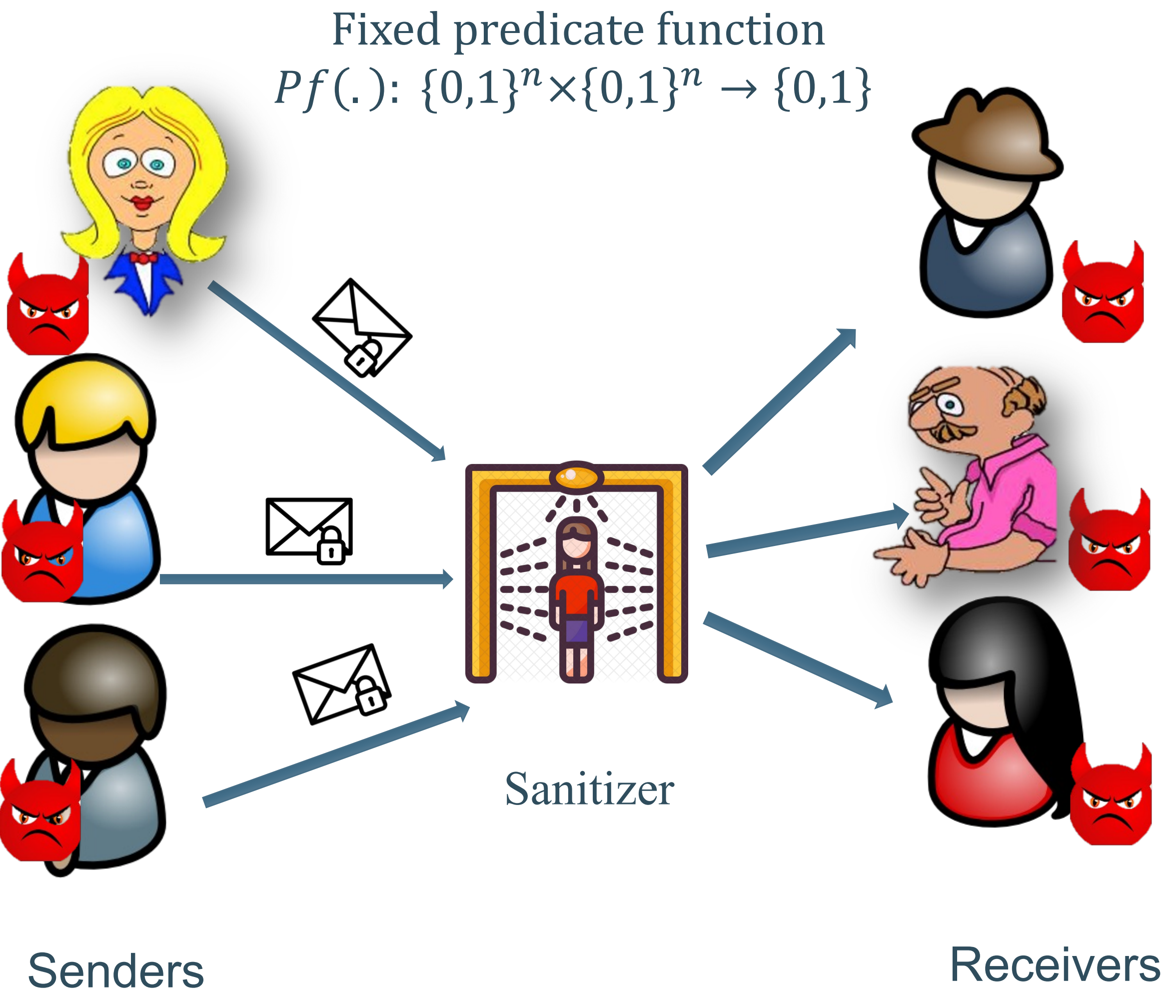
6 : $b \leftarrow\!\$ \{0, 1\}$

7 : $(\mathtt{Ct}_b, \pi_b, \mathsf{x}) \leftarrow\!\$ \mathsf{Enc}(\mathsf{ek}_{\mathbb{P}^*}, m_b)$

8 : $b' \leftarrow\!\$ \mathcal{A}^{\mathcal{O}}(\mathtt{Ct}_b, \pi_b, \mathsf{x})$

Security requirements:

No-Write rule



No-Write rule:

No unauthorized sender can deliver a ciphertext

$\textsc{No-Write}^{\mathcal{A}}_{\text{CD-ABACE}}(1^\lambda, \mathbb{U})$

$$
\begin{aligned}
&1: \quad (\mathsf{pp}_{ra}, \mathsf{msk}_{ra}) \leftarrow \mathsf{RAgen}(1^\lambda, \mathbb{U})\\
&2: \quad (\mathsf{pp}_{sa}, \mathsf{msk}_{sa}) \leftarrow \mathsf{SAgen}(\mathsf{pp}_{ra}, \mathbf{R_L})\\
&3: \quad (\mathtt{Ct}^*, \pi^*, \mathtt{x}^*, \mathbb{P}^*) \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pp}_{ra}, \mathsf{pp}_{sa})\\
&4: \quad (\mathtt{Ct}_0, \pi_0, \mathtt{x}_0) := (\mathtt{Ct}^*, \pi^*, \mathtt{x}^*)\\
&5: \quad (\mathsf{ek}_{\mathbb{P}^*}, \sigma^*, W^*) \leftarrow \mathsf{EncKGen}(\mathbb{P}^*)\\
&6: \quad m^* \leftarrow\$ \mathcal{M}\\
&7: \quad \mathsf{aux} \leftarrow \mathsf{fix}(\mathtt{Ct}_0)\\
&8: \quad (\mathtt{Ct}_1, \pi_1, \mathtt{x}_1) \leftarrow \mathsf{Enc}(\mathsf{ek}_{\mathbb{P}^*}, m^*, \mathsf{aux})\\
&9: \quad b \leftarrow\$ \{0,1\}\\
&10: \quad \tilde{\mathtt{Ct}}_b \leftarrow \mathsf{Sanitization}(\mathtt{Ct}_b, \pi_b, \mathtt{x}_b)\\
&11: \quad b' \leftarrow\$ \mathcal{A}^{\mathcal{O}}(\tilde{\mathtt{Ct}}_b)
\end{aligned}
$$