MILCOM

Military Communications Conference

29 November–2 December 2021
San Diego, CA, USA

IEEE ComSoc®
IEEE Communications Society

AFCEA

Solving the Cross Domain Problem with Functional Encryption

A. Kaminsky, M. Kurdziel*, S. Farris*, M. Łukowiak, S. Radziszowski

Rochester Institute of Technology
*L3Harris Technologies

MILCOM

IEEE ComSoc
IEEE Communications Society

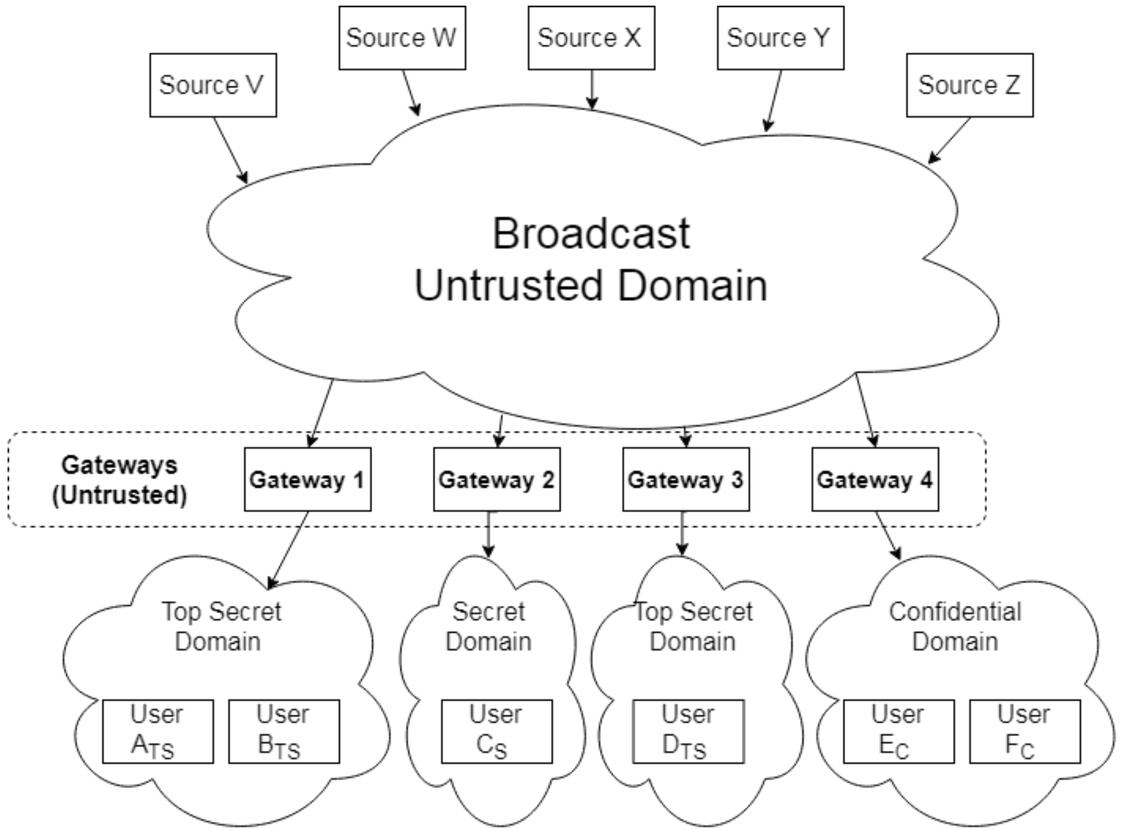
AFCEA

Agenda

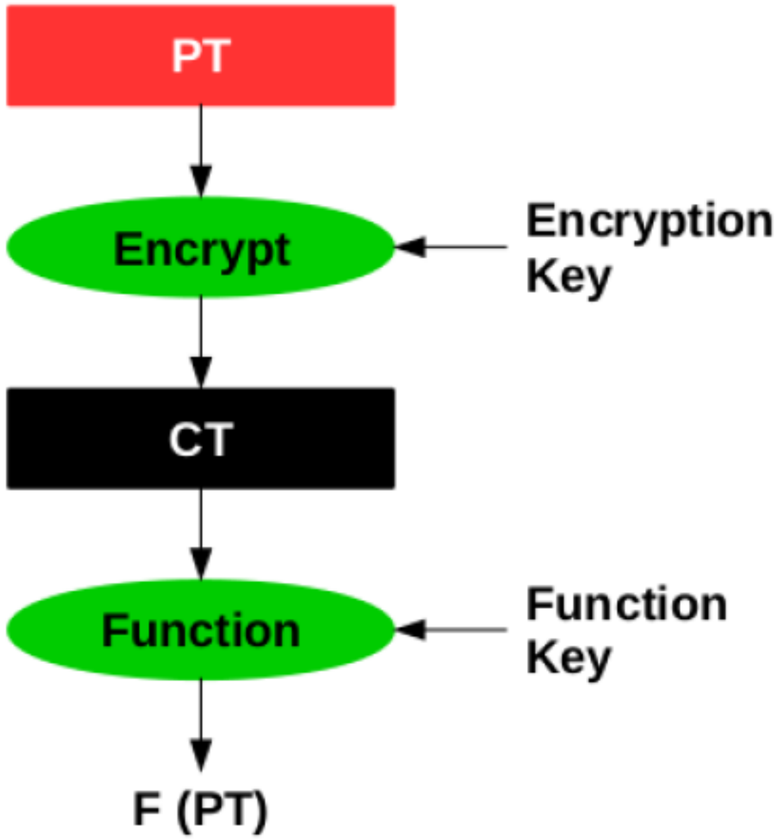
- CDS Problem Statement
- Functional Encryption
- FE: Concealed Attributes
- FE Solution to CDS
- Case Study Implementation
- Results
- Questions

CDS Problem Statement

- Move sensitive content securely *and automatically* from one security domain to another.
- End-to-end encryption can solve the problem.
- Routing classified data through an untrusted network is still a difficult problem.

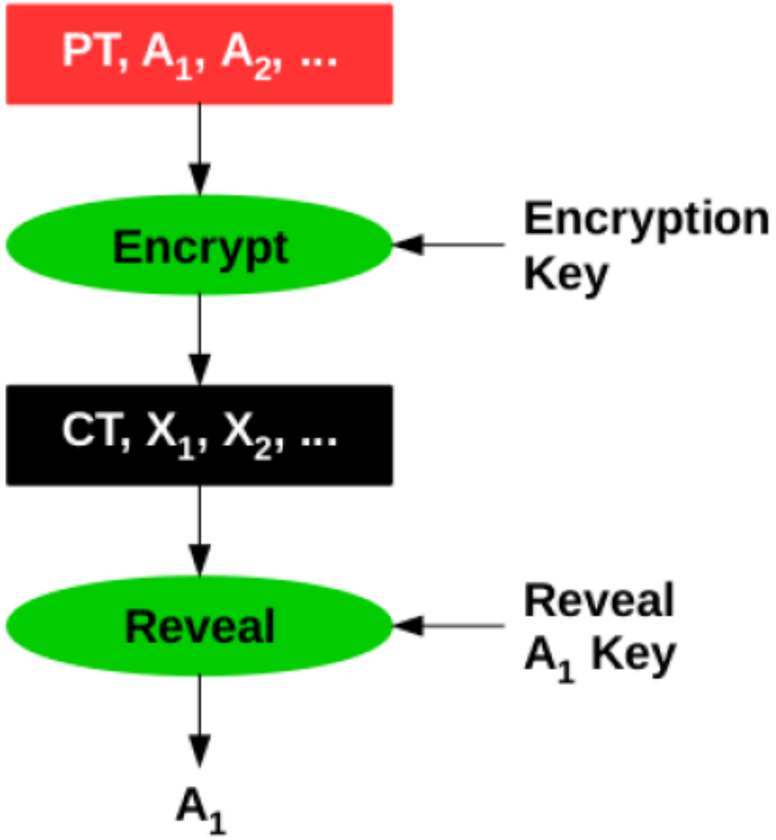


Functional Encryption



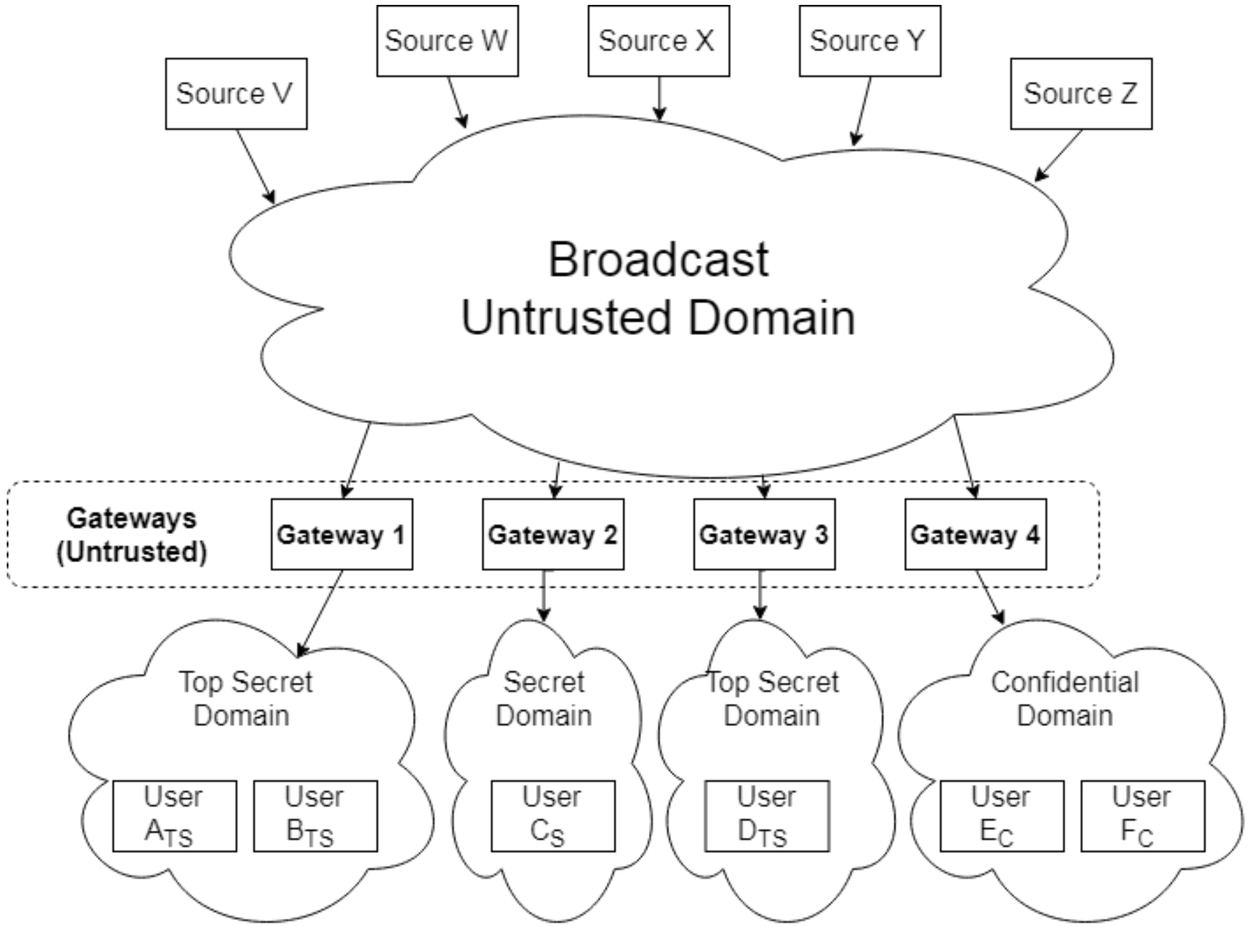
- Examples:
  - Order revealing encryption
  - Searchable encryption
  - Private set intersection

FE: Concealed Attributes



- PT = sensitive content
- A_1, A_2, … = Boolean attributes
- CT = encrypted content
- X_1, X_2, … = concealed attributes
- Given the appropriate key, reveal the value of a particular attribute and nothing else

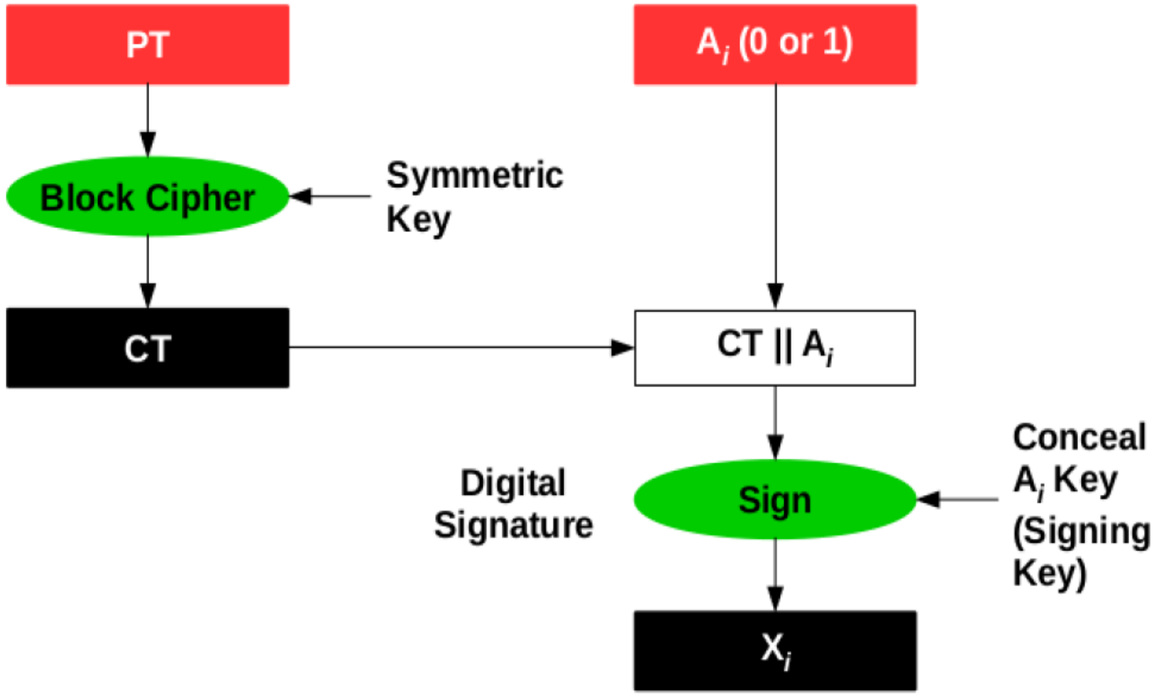
FE Solution to CDS



- PT = sensitive content
- A_i = “routable to security domain i”
- Source encrypts content and all routing attributes
  - Source has encryption key, hence is trusted
- Source broadcasts ciphertext and all concealed attributes
- Each gateway i decrypts with “reveal A_i key”
  - Gateway has reveal A_i key for its security domain only, hence is partially trusted
- A_i = true: gateway forwards message to its security domain
- Otherwise: gateway ignores message

FE Solution to CDS

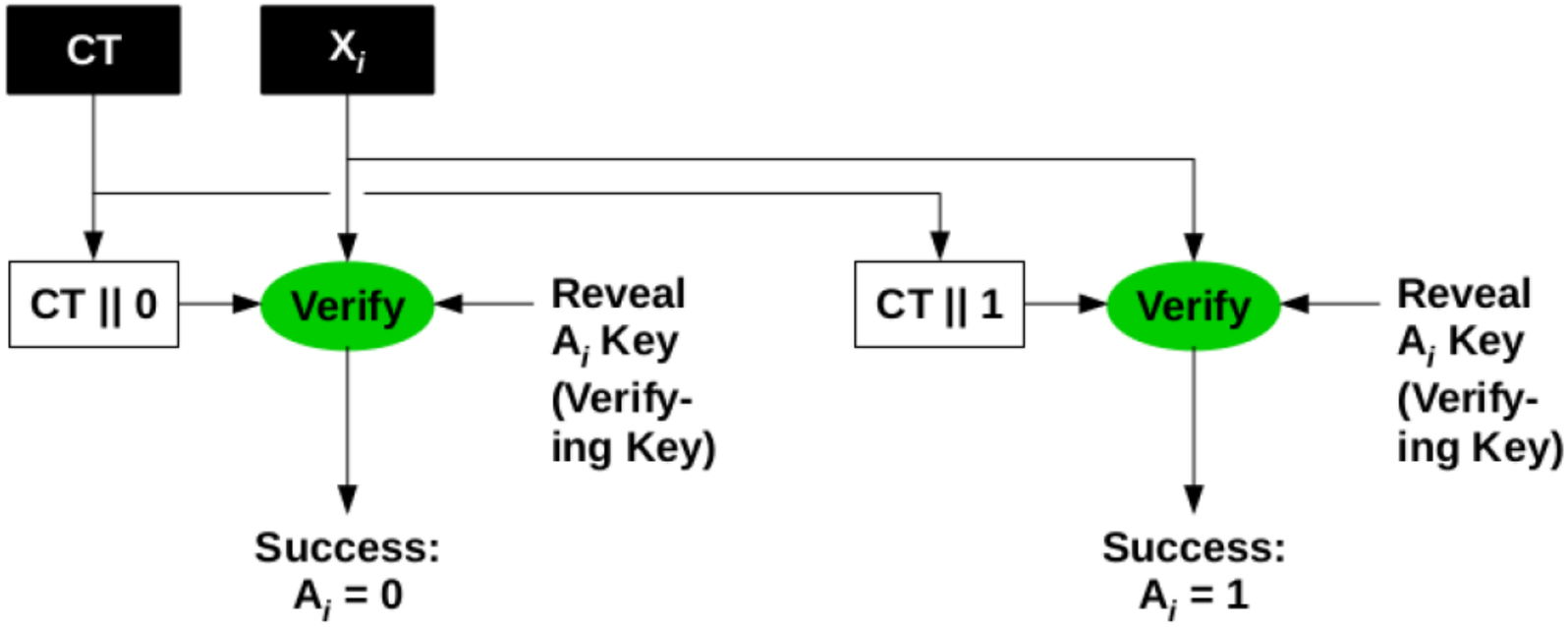
- Attribute concealment



Note: Concealed attribute is bound to its ciphertext

FE Solution to CDS

- Attribute revelation



Note: If both verifications fail, CT, X_i, and/or reveal A_i key is invalid

FE Solution to CDS

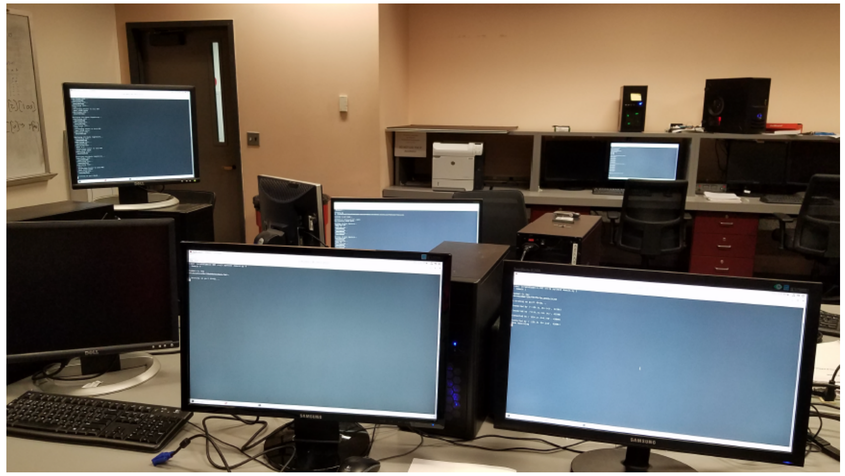
- Gateway cannot
  - Determine plaintext (lacks symmetric key)
  - Determine any attribute value not its own (lacks revealing keys)
  - Forge or alter ciphertext or concealed attributes (lacks concealing keys)
  - Deduce concealing key (digital signature property)

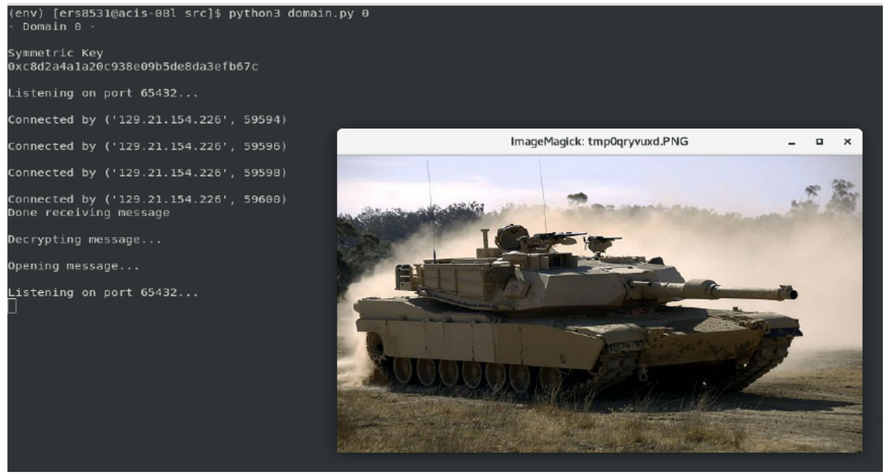
- Intruder cannot
  - Determine plaintext (lacks symmetric key)
  - Determine any attribute value (lacks revealing keys)
  - Forge or alter ciphertext or concealed attributes (lacks concealing keys)

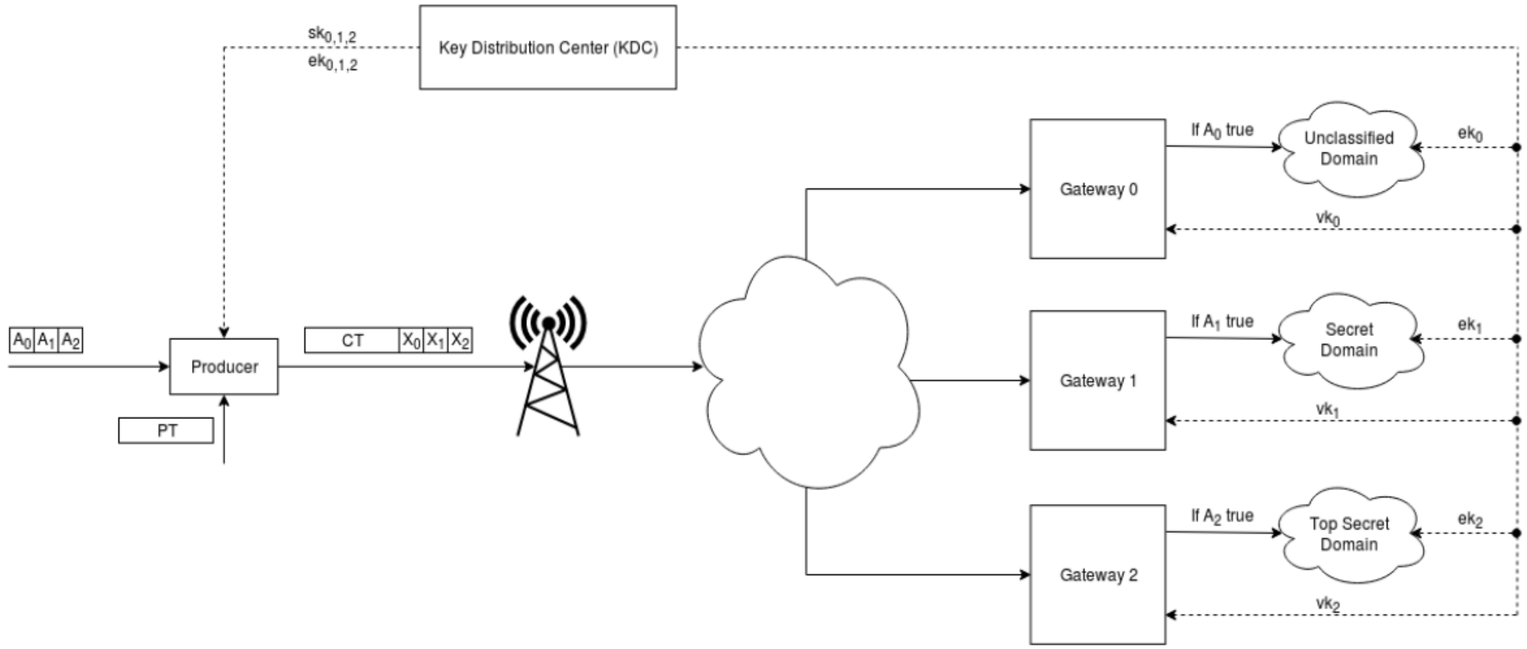
FE Solution to CDS

- Cryptographic protocol that were used:
  - AES GCM (Galois Counter Mode)
    - Encrypts and authenticates secret message
    - 128 bit key
  - ECDSA (Elliptic Curve Digital Signature Algorithm)
    - Signs and verifies attributes
    - NIST curve P-192
    - Each attribute is 48 bytes, increasing message size

Case Study Implementation







Notes:

- Timing measurements were gathered on a PC with AMD Ryzen 5 3600X 6-Core Processor 3.80 GHz, 16.0 GB RAM 2133 MHz, PCIe 4.0 SSD.
- A set of small images was used as PT data and the number of attributes selected for this test was four.
- Python scripts emulate the roles of the Key Distribution Center (KDC), Data Producer, Network Gateways, and Destination Domains.

Results

- Sample case study times for FE based approach

	Time [μs]		
Computation	Producer	Gateway	Domain
AES-GCM encrypt	222		
Signing attributes	1929		
Verifying attributes		5568	
AES-GCM decrypt			521

- Compared to case study times for HE based approach

AVERAGE PERFORMANCE PROFILE RESULTS OF CDS APPLICATION

YASHE configuration	encrypt SIMON key (s)	SIMON key expansion (s)	encrypt metadata (s)	homomorphic SIMON decryption (s)	homomorphic metadata evaluation (s)	decrypt result (s)
α	5.4	112.8	3.2	2433.0	612.0	1.0
β	19.0	419.4	13.3	12149.1	1966.0	3.0
γ	21.4	514.3	13.3	12150.6	1971.2	3.0
δ	78.6	1958.7	48.2	64367.6	8079.1	8.9

Results

- Sample case study times for FE based approach

	Time [μs]		
Computation	Producer	Gateway	Domain
AES-GCM encrypt	222		
Signing attributes	1929		
Verifying attributes		5568	
AES-GCM decrypt			521

- Compared to case study times for HE based approach

AVERAGE PERFORMANCE PROFILE RESULTS OF CDS APPLICATION

YASHE configuration	encrypt SIMON key (s)	SIMON key expansion (s)	encrypt metadata (s)	homomorphic SIMON decryption (s)	homomorphic metadata evaluation (s)	decrypt result (s)
α	5.4	112.8	3.2	2433.0	612.0	1.0
β	19.0	419.4	13.3	12149.1	1966.0	3.0
γ	21.4	514.3	13.3	12150.6	1971.2	3.0
δ	78.6	1958.7	48.2	64367.6	8079.1	8.9

Results

- Sample case study times for FE based approach

	Time [μs]		
Computation	Producer	Gateway	Domain
AES-GCM encrypt	222		
Signing attributes	1929		
Verifying attributes		5568	
AES-GCM decrypt			521

- Compared to case study times for HE based approach

AVERAGE PERFORMANCE PROFILE RESULTS OF CDS APPLICATION

YASHE configuration	encrypt SIMON key (s)	SIMON key expansion (s)	encrypt metadata (s)	homomorphic SIMON decryption (s)	homomorphic metadata evaluation (s)	decrypt result (s)
α	5.4	112.8	3.2	2433.0	612.0	1.0
β	19.0	419.4	13.3	12149.1	1966.0	3.0
γ	21.4	514.3	13.3	12150.6	1971.2	3.0
δ	78.6	1958.7	48.2	64367.6	8079.1	8.9

Questions