Modeling the ISO 9798–2.4 Authentication Protocol

Britta Hale Colin Boyd

Department of Telematics
Norwegian University of Science and Technology

Outline

Outline

1. ISO 9798–2.4

Outline

1. ISO 9798–2.4
2. Analysis Issues

Outline

1. ISO 9798–2.4
2. Analysis Issues
3. Results

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

NTNU
Department of Telematics

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields

NTNU
Department of Telematics

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields
- I_B is a unique identifier

NTNU
Department of Telematics

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields
- I_B is a unique identifier
- $\mathcal{E}$ is an encipherment function

ISO 9798–2.4

$$B \rightarrow A : R_B || Text_1$$

$$A \rightarrow B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \rightarrow A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields
- I_B is a unique identifier
- $\mathcal{E}$ is an encipherment function
- K is a symmetric key

NTNU
Department of Telematics

ISO 9798–2.4

$$B \to A : R_B || Text_1$$

$$A \to B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \to A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields
- I_B is a unique identifier
- $\mathcal{E}$ is an encipherment function
- K is a symmetric key

NTNU
Department of Telematics

ISO 9798–2.4

$$B \to A : R_B || Text_1$$

$$A \to B : Text_3 || \mathcal{E}_K(R_A || R_B || I_B || Text_2)$$

$$B \to A : Text_5 || \mathcal{E}_K(R_B || R_A || Text_4)$$

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- R_i are random nonces
- $Text_j$ are optional text fields
- I_B is a unique identifier
- $\mathcal{E}$ is an encipherment function
- K is a symmetric key

NTNU
Department of Telematics

Past Work

NTNU
Department of Telematics

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"
- A, B believe that they have run the protocol with each other (at some time)

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"
- A, B believe that they have run the protocol with each other (at some time)

Unconsidered:

NTNU
Department of Telematics

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"
- A, B believe that they have run the protocol with each other (at some time)

Unconsidered:

- Selection and properties of the encipherment function

NTNU
Department of Telematics

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"
- A, B believe that they have run the protocol with each other (at some time)

Unconsidered:

- Selection and properties of the encipherment function
- A, B agree on the data exchanged

Past Work

Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther
Secure under:

- Symmetric encryption
- A, B "alive"
- A, B believe that they have run the protocol with each other (at some time)

Unconsidered:

- Selection and properties of the encipherment function
- A, B agree on the data exchanged
- Messages are received in expected order, with data integrity

NTNU
Department of Telematics

Goals

- Encipherment function

Goals

- Encipherment function
- Address optional text fields

NTNU
Department of Telematics

Goals

- Encipherment function
- Address optional text fields
- Computationally prove the security of ISO 9798–2.4

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)
  - Counter with CBC-MAC (CCM)

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)
  - Counter with CBC-MAC (CCM)
  - Key Wrap

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)
  - Counter with CBC-MAC (CCM)
  - Key Wrap
  - EAX (CTR mode for encryption, OMAC for authentication)

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)
  - Counter with CBC-MAC (CCM)
  - Key Wrap
  - EAX (CTR mode for encryption, OMAC for authentication)
  - Encrypt-then-MAC (EtM)

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection
- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity
- ISO/IEC 19772:2009
  - Offset Codebook Mode (OCB)
  - Counter with CBC-MAC (CCM)
  - Key Wrap
  - EAX (CTR mode for encryption, OMAC for authentication)
  - Encrypt-then-MAC (EtM)
  - Galois Counter Mode (GCM)

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

NTNU
Department of Telematics

The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

- Selection for analysis: MAC
  $\mathrm{MAC}_K(M) = (M, \mathit{Tag})$

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$\xrightarrow{R_B}$	
	$\xleftarrow{\mathrm{MAC}_K(R_A, R_B, I_B)}$	
	$\xrightarrow{\mathrm{MAC}_K(R_B, R_A)}$	

ISO 9798–2.4 Protocol Core with $\mathrm{MAC}_K(M) = (M, \mathit{Tag})$

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K Random R_B		Symmetric K Random R_A
	$R_B \| \| Text_1$ $\longrightarrow$	
	$\longleftarrow$ $Text_3 \| \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ $\longrightarrow$	

ISO 9798–2.4 Protocol with $\mathrm{MAC}_K(M) = (M, \textit{Tag})$ and Text Fields

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| \| Text_1$ $\longrightarrow$	
	$\longleftarrow$ $Text_3 \| \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ $\longrightarrow$	

ISO 9798–2.4 Protocol with $\mathrm{MAC}_K(M) = (M, \textit{Tag})$ and Text Fields

No security guarantee on text fields content selection

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| Text_1$ $\longrightarrow$	
	$\longleftarrow$ $Text_3 \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ $\longrightarrow$	

ISO 9798–2.4 Protocol with $\mathrm{MAC}_K(M) = (M, \textit{Tag})$ and Text Fields

No security guarantee on text fields content selection

NTNU
Department of Telematics

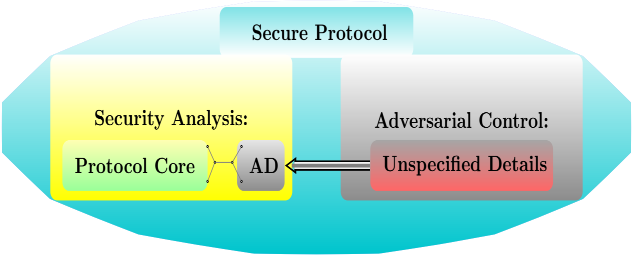
Optional Text Fields

Optional Text Fields

Rogaway and Stegers Framework (2009)

Optional Text Fields

Rogaway and Stegers Framework (2009)



Optional Text Fields

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$\xrightarrow{R_B \| Text_1}$	
	$\xleftarrow{Text_3 \| \text{MAC}_K(R_A, R_B, I_B, Text_2)}$	
	$\xrightarrow{Text_5 \| \text{MAC}_K(R_B, R_A, Text_4)}$	

Which text fields are Associated Data?

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| \| Text_1$ →	
	← $Text_3 \| \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ →	

Which text fields are Associated Data?

$Text_1, Text_3, Text_5$: Unauthenticated

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| \| Text_1$ →	
	← $Text_3 \| \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ →	

Which text fields are Associated Data?

$Text_1, Text_3, Text_5$: Unauthenticated

$Text_2$: Authenticated

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| Text_1$ $\longrightarrow$	
	$Text_3 \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$ $\longleftarrow$	
	$Text_5 \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ $\longrightarrow$	

Which text fields are Associated Data?

$Text_1, Text_3, Text_5$: Unauthenticated

$Text_2$: Authenticated

$Text_4$: Authenticated, but no confirmation message received.

NTNU
Department of Telematics

Optional Text Fields

B		A
Symmetric K		Symmetric K
Random R_B		Random R_A
	$R_B \| \| Text_1$ $\longrightarrow$	
	$\longleftarrow$ $Text_3 \| \| \mathrm{MAC}_K(R_A, R_B, I_B, Text_2)$	
	$Text_5 \| \| \mathrm{MAC}_K(R_B, R_A, Text_4)$ $\longrightarrow$	

Which text fields are Associated Data?

$Text_1, Text_3, Text_5$: Unauthenticated

$Text_2$: Authenticated $\leftarrow$ **AD**

$Text_4$: Authenticated, but no confirmation message received.

NTNU
Department of Telematics

Security of ISO 9798–2.4

Proof of Security

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$

NTNU
Department of Telematics

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model

1. Matching conversations ⇒ acceptance.

NTNU
Department of Telematics

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model

1. Matching conversations $\Rightarrow$ acceptance.
2. Acceptance $\Rightarrow$ matching conversations.

Security of ISO 9798–2.4

Proof of Security

- Use $\mathcal{E}_K(m) = \mathrm{MAC}_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model with RS Framework

1. Matching conversations $\Rightarrow$ acceptance.
2. Acceptance $\Rightarrow$ matching conversations.
3. Matching Conversations $\Rightarrow$ Matching Associated Data.

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results:

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

Number of principals: p

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

Number of principals: p
Number of sessions: S

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

Number of principals: p
Number of sessions: S
Number of allowed adversary queries: q

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

Number of principals: p
Number of sessions: S
Number of allowed adversary queries: q
Security parameter: 1^k

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results:

$$\mathbf{Adv}^{\mathsf{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \mathbf{Adv}_{\Pi}^{\mathrm{MAC}}(F) + q^2/2^{k+1}$$

If $\mathcal{A}$ runs in time t and asks q queries, then F runs in time $t_F \approx t$ and asks $q_F = q$ queries.

Number of principals: p
Number of sessions: S
Number of allowed adversary queries: q
Security parameter: 1^k

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}^{\mathsf{SUF\text{-}CMA}}_{\mathrm{MAC}}(E) \leq \mathbf{Adv}^{\mathsf{SUF\text{-}AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F)$$

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}^{\mathsf{SUF\text{-}CMA}}_{\mathrm{MAC}}(E) \leq \mathbf{Adv}^{\mathsf{SUF\text{-}AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F)$$

Adversarial advantage with associated data considered:

$$\mathbf{Adv}^{\mathsf{MA\text{-}AE}}_{\Pi}(\mathcal{A}) \leq (2p^2S + n) \cdot \mathbf{Adv}^{\mathsf{SUF\text{-}AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F) + q^2/2^{k+1}$$

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}^{\text{SUF-CMA}}_{\mathrm{MAC}}(E) \leq \mathbf{Adv}^{\text{SUF-AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F)$$

Adversarial advantage with associated data considered:

$$\mathbf{Adv}^{\text{MA-AE}}_{\Pi}(\mathcal{A}) \leq (2p^2S + n) \cdot \mathbf{Adv}^{\text{SUF-AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F) + q^2/2^{k+1}$$

Strongly unforgeable authenticated encryption (SUF-AE) algorithm

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}_{\mathrm{MAC}}^{\text{SUF-CMA}}(E) \leq \mathbf{Adv}_{(\mathcal{K},\mathcal{E},\mathcal{D})}^{\text{SUF-AE}}(F)$$

Adversarial advantage with associated data considered:

$$\mathbf{Adv}_{\Pi}^{\text{MA-AE}}(\mathcal{A}) \leq (2p^2S + n) \cdot \mathbf{Adv}_{(\mathcal{K},\mathcal{E},\mathcal{D})}^{\text{SUF-AE}}(F) + q^2/2^{k+1}$$

Strongly unforgeable authenticated encryption (SUF-AE) algorithm
Number of allowed queries for MA-AE adversary $\mathcal{A}$: n

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}^{\mathsf{SUF\text{-}CMA}}_{\mathrm{MAC}}(E) \leq \mathbf{Adv}^{\mathsf{SUF\text{-}AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F)$$

Adversarial advantage with associated data considered:

$$\mathbf{Adv}^{\mathsf{MA\text{-}AE}}_{\Pi}(\mathcal{A}) \leq (2p^2S + n) \cdot \mathbf{Adv}^{\mathsf{SUF\text{-}AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F) + q^2/2^{k+1}$$

Strongly unforgeable authenticated encryption (SUF-AE) algorithm
Number of allowed queries for MA-AE adversary $\mathcal{A}$: n
Number of allowed queries for MA-MAC adversary: q

NTNU
Department of Telematics

Security of ISO 9798–2.4

Results with Authenticated Encryption:

Consider: $\mathrm{MAC}_K(M) = (M, \mathsf{AE}(K, M))$

SUF-AE:

$$\mathbf{Adv}^{\text{SUF-CMA}}_{\mathrm{MAC}}(E) \leq \mathbf{Adv}^{\text{SUF-AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F)$$

Adversarial advantage with associated data considered:

$$\mathbf{Adv}^{\text{MA-AE}}_{\Pi}(\mathcal{A}) \leq (2p^2 S + n) \cdot \mathbf{Adv}^{\text{SUF-AE}}_{(\mathcal{K},\mathcal{E},\mathcal{D})}(F) + q^2/2^{k+1}$$

Strongly unforgeable authenticated encryption (SUF-AE) algorithm
Number of allowed queries for MA-AE adversary $\mathcal{A}$: n
Number of allowed queries for MA-MAC adversary: q

NTNU
Department of Telematics

Questions?