Modeling the ISO 9798–2.4 Authentication Protocol

Britta Hale  Colin Boyd

Department of Telematics  
Norwegian University of Science and Technology
Computationally Analyzing the ISO 9798–2.4 Authentication Protocol

Outline

1. ISO 9798–2.4
2. Analysis Issues
Outline

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

\[
B \rightarrow A : R_B || Text_1
\]

\[
A \rightarrow B : Text_3 || E_K(R_A || R_B || I_B || Text_2)
\]

\[
B \rightarrow A : Text_5 || E_K(R_B || R_A || Text_4)
\]

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol
ISO 9798–2.4

\[ B \rightarrow A : R_B || \text{Text}_1 \]

\[ A \rightarrow B : \text{Text}_3 || E_K(R_A || R_B || I_B || \text{Text}_2) \]

\[ B \rightarrow A : \text{Text}_5 || E_K(R_B || R_A || \text{Text}_4) \]

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

- \( R_i \) are random nonces
ISO 9798–2.4

Computationally Analyzing the ISO 9798–2.4 Authentication Protocol

ISO 9798–2 Mechanism 4 Mutual Authentication Protocol

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

\[
B \rightarrow A : R_B || Text_1
\]

\[
A \rightarrow B : Text_3 || E_K(R_A || R_B || I_B || Text_2)
\]

\[
B \rightarrow A : Text_5 || E_K(R_B || R_A || Text_4)
\]
ISO 9798–2.4

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

$B \rightarrow A : R_B | \text{Text}_1$

$A \rightarrow B : \text{Text}_3 | \mathcal{E}_K(R_A | R_B | I_B | \text{Text}_2)$

$B \rightarrow A : \text{Text}_5 | \mathcal{E}_K(R_B | R_A | \text{Text}_4)$
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
- $E$ is an encipherment function
ISO 9798–2.4 Mutual Authentication Protocol

\[ B \rightarrow A : R_B || Text_1 \]

\[ A \rightarrow B : Text_3 || E_K(R_A || R_B || I_B || Text_2) \]

\[ B \rightarrow A : Text_5 || E_K(R_B || R_A || Text_4) \]

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
- \( E \) is an encipherment function
- \( K \) is a symmetric key
ISO 9798–2.4

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
Computationally Analyzing the ISO 9798–2.4 Authentication Protocol

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
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
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:

• Symmetric encryption
• $A, B$ "alive"
• $A, B$ agree on the data exchanged
• Messages are received in expected order, with data integrity
Basin, Cremers, Meier (2012) ISO 9798–2.4 analysis using Scyther Secure under:

- Symmetric encryption
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:
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
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
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
GOALS

- Encipherment function
Goals

- Encipherment function
- Address optional text fields
Goals

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

- Standard properties:
  Integrity and Manipulation Detection
The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

- Standard: Authenticated Encryption
The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

- **Standard: Authenticated Encryption**
  What is authenticated encryption?
The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

- **Standard: Authenticated Encryption**
  What is authenticated encryption?
  - Confidentiality
The Encipherment Function

- Standard properties: Integrity and Manipulation Detection

- **Standard: Authenticated Encryption**
  What is authenticated encryption?
  - Confidentiality
  - Integrity
The Encipherment Function

- Standard properties: Integrity and Manipulation Detection

- Standard: Authenticated Encryption
  What is authenticated encryption?
  - Confidentiality
  - Integrity

- ISO/IEC 19772:2009
Standard properties:
- Integrity and Manipulation Detection

Standard: Authenticated Encryption
What is authenticated encryption?
- Confidentiality
- Integrity

ISO/IEC 19772:2009
- Offset Codebook Mode (OCB)
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)
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
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)
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
The Encipherment Function

- Standard properties:
  Integrity and Manipulation Detection

- Selection for analysis: MAC
  \[ MAC_K(M) = (M, \text{Tag}) \]
ISO 9798–2.4 Protocol Core with $\text{MAC}_K(M) = (M, \text{Tag})$
ISO 9798–2.4 Protocol with $\text{MAC}_K(M) = (M, \text{Tag})$ and Text Fields
ISO 9798–2.4 Protocol with $MAC_K(M) = (M, Tag)$ and Text Fields

No security guarantee on text fields content selection
Optional Text Fields

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

No security guarantee on text fields content selection
Rogaway and Stegers Framework (2009)
Rogaway and Stegers Framework (2009)
**Optional Text Fields**

Computationally Analyzing the ISO 9798–2.4 Authentication Protocol

---

Text 1 \[\rightarrow^{\text{MAC}}_{K}(R_{A}, R_{B}, I_{B})\]

Text 2

Text 3

Text 4 \[\rightarrow^{\text{MAC}}_{K}(R_{B}, R_{A})\]

Text 5

Which text fields are Associated Data?

Unauthenticated, but no confirmation message received.
\begin{align*}
B & \quad \text{Symmetric } K \\
\text{Random } R_B & \\
\hline
R_B \| \text{Text}_1 & \\
\hline
\text{Text}_3 \| \text{MAC}_K(R_A, R_B, I_B, \text{Text}_2) & \\
\hline
\text{Text}_5 \| \text{MAC}_K(R_B, R_A, \text{Text}_4) & \quad A \\
\text{Symmetric } K \\
\text{Random } R_A &
\end{align*}

Which text fields are Associated Data?
Which text fields are Associated Data?

\(\text{Text}_1, \text{Text}_3, \text{Text}_5: \text{Unauthenticated}\)
Computationally Analyzing the ISO 9798–2.4 Authentication Protocol

Optional Text Fields

<table>
<thead>
<tr>
<th>B</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric ( K )</td>
<td>Symmetric ( K )</td>
</tr>
<tr>
<td>Random ( R_B )</td>
<td>Random ( R_A )</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
R_B || Text_1 & \\
\text{Text}_3 || \text{MAC}_K(R_A, R_B, I_B, \text{Text}_2) & \\
\text{Text}_5 || \text{MAC}_K(R_B, R_A, \text{Text}_4) & 
\end{align*}
\]

Which text fields are Associated Data?

\( \text{Text}_1, \text{Text}_3, \text{Text}_5 \): Unauthenticated

\( \text{Text}_2 \): Authenticated
Optional Text Fields

\[
\begin{align*}
B & \quad \text{Symmetric } K \\
\text{Random } R_B & \\
\end{align*}
\]

\[
\begin{align*}
R_B || Text_1 & \\
\downarrow & \\
Text_3 || \text{MAC}_K(R_A, R_B, I_B, Text_2) & \\
\leftarrow & \\
Text_5 || \text{MAC}_K(R_B, R_A, Text_4) & \\
\end{align*}
\]

\[
\begin{align*}
A & \quad \text{Symmetric } K \\
\text{Random } R_A & \\
\end{align*}
\]

Which text fields are Associated Data?

\[
\begin{align*}
Text_1, Text_3, Text_5: & \quad \text{Unauthenticated} \\
Text_2: & \quad \text{Authenticated} \\
Text_4: & \quad \text{Authenticated, but no confirmation message received.}
\end{align*}
\]
Which text fields are Associated Data?

\( \text{Text}_1, \text{Text}_3, \text{Text}_5 \): Unauthenticated

\( \text{Text}_2 \): Authenticated \( \leftarrow \) AD

\( \text{Text}_4 \): Authenticated, but no confirmation message received.
Proof of Security
**Security of ISO 9798–2.4**

Proof of Security

- Use $E_K(m) = MAC_K(m)$ (SUF-CMA)
Proof of Security

- Use $E_K(m) = MAC_K(m)$ (SUF-CMA)

- Associated data: $Text_2$
Proof of Security

- Use $E_K(m) = MAC_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$
Proof of Security

- Use $E_K(m) = MAC_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model
Proof of Security

- Use $E_K(m) = MAC_K(m)$ (SUF-CMA)
- Associated data: $Text_2$
- Authenticated but unassociated data: $Text_4$

Bellare–Rogaway Mutual Authentication Model

1. Matching conversations $\Rightarrow$ acceptance.
Security of ISO 9798–2.4

Proof of Security

- Use $E_K(m) = MAC_K(m)$ (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.
Proof of Security

- Use $E_K(m) = MAC_K(m)$ (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.
Results:
Results:

$$\text{Adv}^\text{MA}(A) \leq 2p^2S \cdot \text{Adv}_\Pi^\text{MAC}(F) + q^2/2^{k+1}$$
Results:

\[ \text{Adv}^{\text{MA}}(\mathcal{A}) \leq 2p^2S \cdot \text{Adv}^{\text{MAC}}(\mathcal{F}) + q^2/2^{k+1} \]

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

\[ \text{Adv}^{\text{MA}}(A) \leq 2p^2S \cdot \text{Adv}^{\text{MAC}}(F) + q^2/2^{k+1} \]

If \( A \) 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: \( p \)
Results:

\[ \text{Adv}^{\text{MA}}(A) \leq 2p^2 S \cdot \text{Adv}^{\text{MAC}}(F) + \frac{q^2}{2^k+1} \]

If \( A \) 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: \( S \)
Results:

\[ \text{Adv}^{\text{MA}}(A) \leq 2p^2S \cdot \text{Adv}^{\text{MAC}}_\Pi(F) + \frac{q^2}{2^{k+1}} \]

If \( A \) 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: \( q \)
Results:

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

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: $1^k$
Results:

\[
\text{Adv}^{\text{MA}}(\mathcal{A}) \leq 2p^2 S \cdot \text{Adv}^{\text{MAC}}_{\Pi}(F) + q^2 / 2^{k+1}
\]

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: \( 1^k \)
Results with Authenticated Encryption:

Consider: $MAC_K(M) = (M, AE(K, M))$
Results with Authenticated Encryption:
Consider: $\text{MAC}_K(M) = (M, \text{AE}(K, M))$

SUF-AE:

$$\text{Adv}^{\text{SUF-CMA}}_{\text{MAC}}(E) \leq \text{Adv}^{\text{SUF-AE}}_{(K, \varepsilon, D)}(F')$$
Results with Authenticated Encryption:
Consider: $\text{MAC}_K(M) = (M, \text{AE}(K, M))$

SUF-AE:

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

Adversarial advantage with associated data considered:

$\text{Adv}^\text{MA-AE}_{\Pi}(\mathcal{A}) \leq (2p^2S + n) \cdot \text{Adv}^\text{SUF-AE}_{(\mathcal{K}, \mathcal{E}, \mathcal{D})}(F') + q^2/2^{k+1}$
Results with Authenticated Encryption:
Consider: $\text{MAC}_K(M) = (M, \text{AE}(K, M))$

SUF-AE:

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

Adversarial advantage with associated data considered:

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

Strongly unforgeable authenticated encryption (SUF-AE) algorithm
Security of ISO 9798–2.4

Results with Authenticated Encryption:
Consider: $MAC_K(M) = (M, AE(K, M))$

SUF-AE:

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

Adversarial advantage with associated data considered:

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

Strongly unforgeable authenticated encryption (SUF-AE) algorithm
Number of allowed queries for MA-AE adversary $A$: $n$
**Security of ISO 9798–2.4**

**Results with Authenticated Encryption:**

Consider: \( \text{MAC}_K(M) = (M, \text{AE}(K, M)) \)

**SUF-AE:**

\[
\text{Adv}^{\text{SUF-CMA}}(E) \leq \text{Adv}^{\text{SUF-AE}}(K, E, D)(F')
\]

Adversarial advantage with associated data considered:

\[
\text{Adv}^{\text{MA-AE}}(A) \leq (2p^2S + n) \cdot \text{Adv}^{\text{SUF-AE}}(K, E, D)(F') + q^2/2^{k+1}
\]

**Strongly unforgeable authenticated encryption (SUF-AE) algorithm**

Number of allowed queries for MA-AE adversary \( A \): \( n \)

Number of allowed queries for MA-MAC adversary: \( q \)
**Results with Authenticated Encryption:**

Consider: \( \text{MAC}_K(M) = (M, \text{AE}(K, M)) \)

**SUF-AE:**

\[
\text{Adv}^{\text{SUF-CMA}}_{\text{MAC}}(E) \leq \text{Adv}^{\text{SUF-AE}}_{(K,\mathcal{E},\mathcal{D})}(F')
\]

Adversarial advantage with associated data considered:

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

Strongly unforgeable authenticated encryption (SUF-AE) algorithm

Number of allowed queries for MA-AE adversary \( A \): \( n \)

Number of allowed queries for MA-MAC adversary: \( q \)
Questions?