

Universally Composable Signcryption

Kristian Gjøsteen and Lillian Kråkmo

Department of Mathematical Sciences
Norwegian University of Science and Technology

June 26, 2007

How can we convince ourselves that a protocol is secure?

How can we convince ourselves that a protocol is secure?

- Traditionally, protocols have been analyzed in a stand-alone setting.

How can we convince ourselves that a protocol is secure?

- Traditionally, protocols have been analyzed in a stand-alone setting.
- In modern networks, protocols are run concurrently with arbitrary other protocols.

How can we convince ourselves that a protocol is secure?

- Traditionally, protocols have been analyzed in a stand-alone setting.
- In modern networks, protocols are run concurrently with arbitrary other protocols.
- Unfortunately, security in the stand-alone setting does not imply security under protocol composition.

- This framework defines security in such a way that secure protocols remain secure within any context, and allows for a modular design and analysis of complex protocols.

Universally Composable Security (Canetti 01)

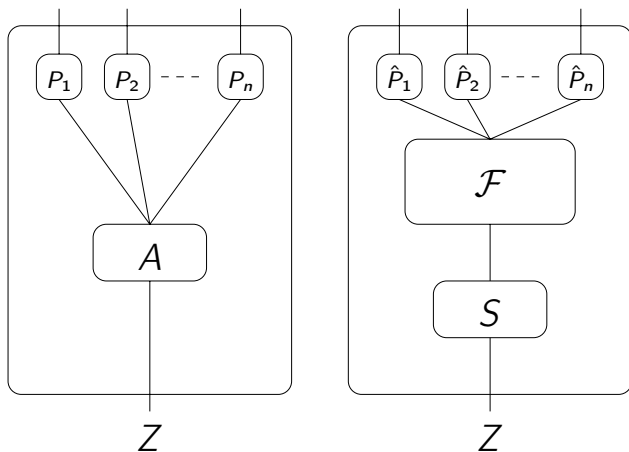
- This framework defines security in such a way that secure protocols remain secure within any context, and allows for a modular design and analysis of complex protocols.
- How is security defined?

Universally Composable Security (Canetti 01)

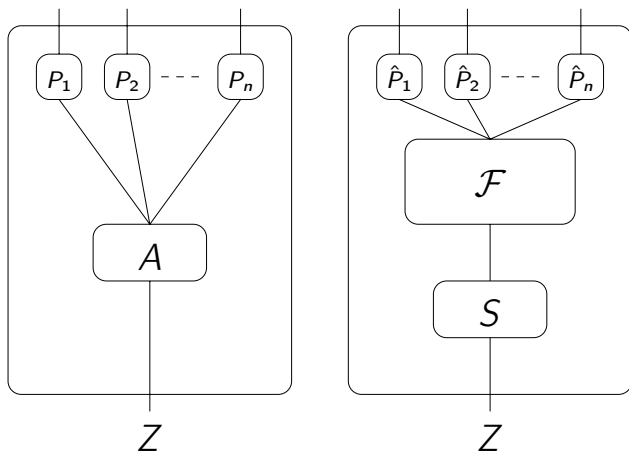
- This framework defines security in such a way that secure protocols remain secure within any context, and allows for a modular design and analysis of complex protocols.
- How is security defined?
 - For each cryptographic task, an **ideal functionality** can be defined, incorporating the required properties of a protocol and the allowed actions of an adversary.

- This framework defines security in such a way that secure protocols remain secure within any context, and allows for a modular design and analysis of complex protocols.
- How is security defined?
 - For each cryptographic task, an **ideal functionality** can be defined, incorporating the required properties of a protocol and the allowed actions of an adversary.
 - Informally, a protocol is said to **securely realize** the functionality, if any effect caused by an adversary attacking the protocol can be obtained by an adversary attacking the ideal functionality.

The real protocol π and the ideal protocol $\text{IDEAL}_{\mathcal{F}}$



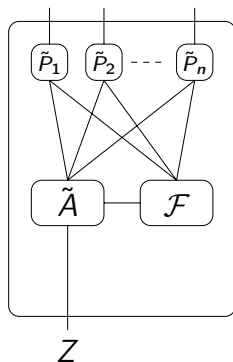
The real protocol π and the ideal protocol $\text{IDEAL}_{\mathcal{F}}$



- We say that π **securely realizes** \mathcal{F} if, for all adversaries A , there exists an ideal adversary S such that no environment Z can tell whether it is interacting with A and π or S and $\text{IDEAL}_{\mathcal{F}}$.

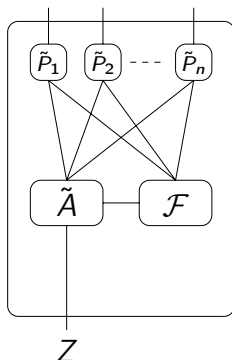
The Composition Theorem

- The hybrid protocol $\tilde{\pi}$



The Composition Theorem

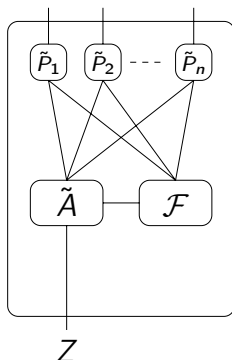
- The hybrid protocol $\tilde{\pi}$



- Assume that a protocol π realizes \mathcal{F} , and that $\tilde{\pi}(\pi)$ is the protocol $\tilde{\pi}$ where \mathcal{F} is replaced by π .

The Composition Theorem

- The hybrid protocol $\tilde{\pi}$



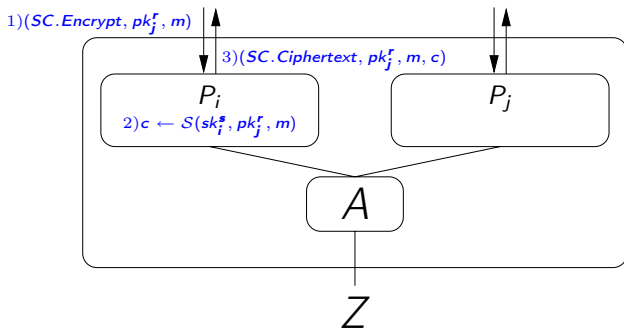
- Assume that a protocol π realizes \mathcal{F} , and that $\tilde{\pi}(\pi)$ is the protocol $\tilde{\pi}$ where \mathcal{F} is replaced by π .
- The composition theorem then says that if $\tilde{\pi}$ securely realizes an ideal functionality \mathcal{G} , then $\tilde{\pi}(\pi)$ also securely realizes \mathcal{G} .

→ confidentiality and authenticity in a single step

Signcryption (Zheng 97)

→ confidentiality and authenticity in a single step

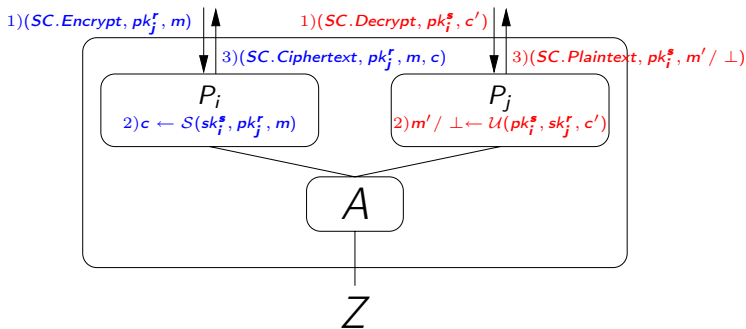
- The signcryption protocol π_{SC}



Signcryption (Zheng 97)

→ confidentiality and authenticity in a single step

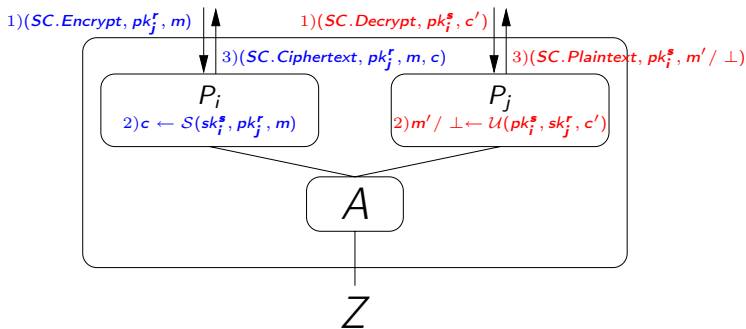
- The signcryption protocol π_{SC}



Signcryption (Zheng 97)

→ confidentiality and authenticity in a single step

- The signcryption protocol π_{SC}



- How should we define the ideal functionality \mathcal{F}_{SC} ?

- Confidentiality:

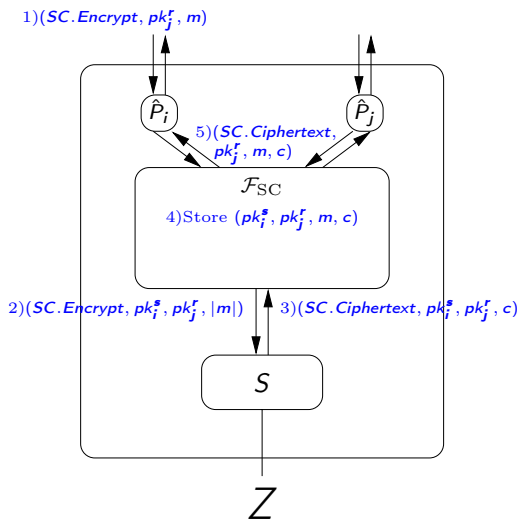
- Confidentiality:
 - **Indistinguishability (IND)**: An adversary who chooses two messages, m_0 and m_1 , cannot later distinguish an encryption of m_0 from an encryption of m_1 .

- Confidentiality:
 - **Indistinguishability (IND)**: An adversary who chooses two messages, m_0 and m_1 , cannot later distinguish an encryption of m_0 from an encryption of m_1 .
 - **Real-or-random (ROR)**: An adversary who chooses a message m cannot later distinguish an encryption of m from an encryption of a hidden random string.

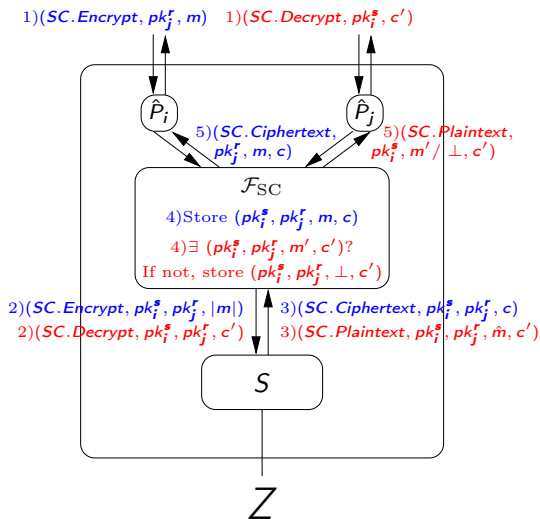
- Confidentiality:
 - **Indistinguishability (IND)**: An adversary who chooses two messages, m_0 and m_1 , cannot later distinguish an encryption of m_0 from an encryption of m_1 .
 - **Real-or-random (ROR)**: An adversary who chooses a message m cannot later distinguish an encryption of m from an encryption of a hidden random string.
 - We can prove: **IND-CCA2** \Leftrightarrow **ROR-CCA2**

- Confidentiality:
 - **Indistinguishability (IND)**: An adversary who chooses two messages, m_0 and m_1 , cannot later distinguish an encryption of m_0 from an encryption of m_1 .
 - **Real-or-random (ROR)**: An adversary who chooses a message m cannot later distinguish an encryption of m from an encryption of a hidden random string.
 - We can prove: **IND-CCA2** \Leftrightarrow **ROR-CCA2**
- Authenticity: **EXT-CMA**

The ideal protocol $\text{IDEAL}_{\mathcal{F}_{\text{SC}}}$



The ideal protocol $\text{IDEAL}_{\mathcal{F}_{\text{SC}}}$



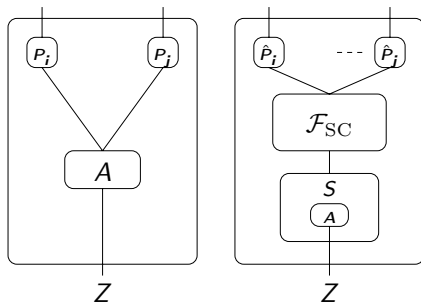
- We can prove: A signcryption scheme \mathcal{SC} is secure with respect to IND-CCA2 and EXT-CMA \Leftrightarrow the protocol $\pi_{\mathcal{SC}}$ securely realizes $\mathcal{F}_{\mathcal{SC}}$.

- We can prove: A signcryption scheme \mathcal{SC} is secure with respect to IND-CCA2 and EXT-CMA \Leftrightarrow the protocol $\pi_{\mathcal{SC}}$ securely realizes $\mathcal{F}_{\mathcal{SC}}$.
- Proof strategy (\Rightarrow):

- We can prove: A signcryption scheme \mathcal{SC} is secure with respect to IND-CCA2 and EXT-CMA \Leftrightarrow the protocol $\pi_{\mathcal{SC}}$ securely realizes $\mathcal{F}_{\mathcal{SC}}$.
- Proof strategy (\Rightarrow):
 - Construct an ideal adversary S .

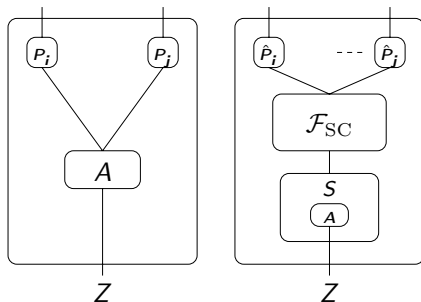
- We can prove: A signcryption scheme \mathcal{SC} is secure with respect to IND-CCA2 and EXT-CMA \Leftrightarrow the protocol $\pi_{\mathcal{SC}}$ securely realizes $\mathcal{F}_{\mathcal{SC}}$.
- Proof strategy (\Rightarrow):
 - Construct an ideal adversary S .
 - Assume that there exists an environment Z that can tell whether it is interacting with A and $\pi_{\mathcal{SC}}$ or S and $\text{IDEAL}_{\mathcal{F}_{\mathcal{SC}}}$, and construct an adversary breaking the IND-CCA2-security or an adversary breaking the EXT-CMA-security of the scheme.

Proof sketch (\Rightarrow)



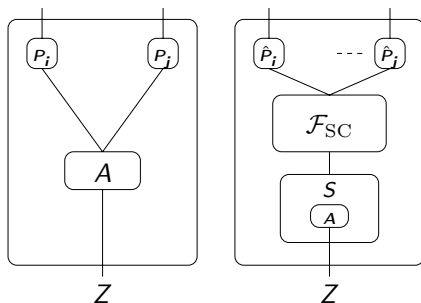
- S runs a simulated copy of A , and encrypts and decrypts using the algorithms \mathcal{S} and \mathcal{U} , just like P_i and P_j in the real protocol.

Proof sketch (\Rightarrow)



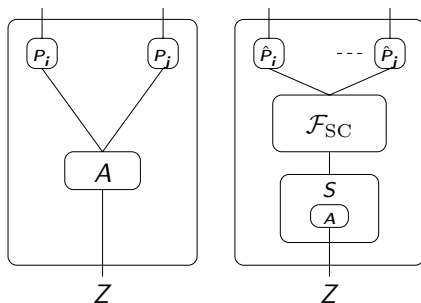
- S runs a simulated copy of A , and encrypts and decrypts using the algorithms \mathcal{S} and \mathcal{U} , just like P_i and P_j in the real protocol.
- What separates π_{SC} from $\text{IDEAL}_{\mathcal{F}_{SC}}$?

Proof sketch (\Rightarrow)



- S runs a simulated copy of A , and encrypts and decrypts using the algorithms \mathcal{S} and \mathcal{U} , just like P_i and P_j in the real protocol.
- What separates π_{SC} from $\text{IDEAL}_{\mathcal{F}_{SC}}$?
 - 1 In π_{SC} the **real message** is encrypted, while in $\text{IDEAL}_{\mathcal{F}_{SC}}$ S only knows the length of the message, and encrypts a **random message**.

Proof sketch (\Rightarrow)



- S runs a simulated copy of A , and encrypts and decrypts using the algorithms \mathcal{S} and \mathcal{U} , just like P_i and P_j in the real protocol.
- What separates π_{SC} from $\text{IDEAL}_{\mathcal{F}_{SC}}$?
 - 1 In π_{SC} the **real message** is encrypted, while in $\text{IDEAL}_{\mathcal{F}_{SC}}$ S only knows the length of the message, and encrypts a **random message**.
 - 2 If \hat{P}_j is asked to decrypt a valid ciphertext that has not been produced by \hat{P}_i , the **decryption** will be output in π_{SC} , while \perp will be output in $\text{IDEAL}_{\mathcal{F}_{SC}}$.

We define a series of games:

We define a series of games:

Game 0: Z interacts with π_{SC} .

We define a series of games:

Game 0: Z interacts with π_{SC} .

Game 1: As Game 0, except we simulate the honest players P_1, P_2, \dots, P_k .

We define a series of games:

Game 0: Z interacts with π_{SC} .

Game 1: As Game 0, except we simulate the honest players P_1, P_2, \dots, P_k .

Note: From Z 's point of view, there is no difference between Game 0 and Game 1.

We define a series of games:

Game 0: Z interacts with π_{SC} .

Game 1: As Game 0, except we simulate the honest players P_1, P_2, \dots, P_k .

Note: From Z 's point of view, there is no difference between Game 0 and Game 1.

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

We define a series of games:

Game 0: Z interacts with π_{SC} .

Game 1: As Game 0, except we simulate the honest players P_1, P_2, \dots, P_k .

Note: From Z 's point of view, there is no difference between Game 0 and Game 1.

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

We can prove: If Z can distinguish Game 2 from Game 1, we can construct an adversary that breaks the EXT-CMA-security of SC .

Recall:

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

Proof sketch continued

Recall:

- Game 2:** As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .
- Game 3:** As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

Recall:

- Game 2:** As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .
- Game 3:** As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

We can prove: **If Z can distinguish Game 3 from Game 2, we can construct an adversary that breaks the ROR-CCA2-security of \mathcal{SC} .**

Proof sketch continued

Recall:

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

Game 3: As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

We can prove: **If Z can distinguish Game 3 from Game 2, we can construct an adversary that breaks the ROR-CCA2-security of \mathcal{SC} .**

Game 4: As Game 3, except when P_1 encrypts a message for P_3 , a **random message** is encrypted.

⋮

Proof sketch continued

Recall:

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

Game 3: As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

We can prove: **If Z can distinguish Game 3 from Game 2, we can construct an adversary that breaks the ROR-CCA2-security of \mathcal{SC} .**

Game 4: As Game 3, except when P_1 encrypts a message for P_3 , a **random message** is encrypted.

\vdots

Game N-1: As Game N-2, except when P_k encrypts a message for P_{k-1} , a **random message** is encrypted.

Proof sketch continued

Recall:

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

Game 3: As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

We can prove: **If Z can distinguish Game 3 from Game 2, we can construct an adversary that breaks the ROR-CCA2-security of \mathcal{SC} .**

Game 4: As Game 3, except when P_1 encrypts a message for P_3 , a **random message** is encrypted.

\vdots

Game N-1: As Game N-2, except when P_k encrypts a message for P_{k-1} , a **random message** is encrypted.

Game N: Z interacts with $IDEAL_{\mathcal{F}_{SC}}$.

Proof sketch continued

Recall:

Game 2: As Game 1, except if P_j is asked to decrypt a valid ciphertext that has not been produced by P_i , we output \perp .

Game 3: As Game 2, except when P_1 encrypts a message for P_2 , a **random message** is encrypted.

We can prove: **If Z can distinguish Game 3 from Game 2, we can construct an adversary that breaks the ROR-CCA2-security of \mathcal{SC} .**

Game 4: As Game 3, except when P_1 encrypts a message for P_3 , a **random message** is encrypted.

\vdots

Game N-1: As Game N-2, except when P_k encrypts a message for P_{k-1} , a **random message** is encrypted.

Game N: Z interacts with $IDEAL_{\mathcal{F}_{SC}}$.

Note: **From Z 's point of view, there is no difference between Game N-1 and Game N!**

- Hybrid argument: If Z can distinguish Game 0 from Game N , there exists an i , $0 \leq i < N$, such that Z distinguish Game i from Game $i + 1$.

- Hybrid argument: If Z can distinguish Game 0 from Game N , there exists an i , $0 \leq i < N$, such that Z distinguish Game i from Game $i + 1$.
- We have shown that if such an i exists, then there exists an adversary breaking the assumed security of \mathcal{SC} .

- Hybrid argument: If Z can distinguish Game 0 from Game N , there exists an i , $0 \leq i < N$, such that Z distinguish Game i from Game $i + 1$.
- We have shown that if such an i exists, then there exists an adversary breaking the assumed security of \mathcal{SC} .
- Conclusion: $\pi_{\mathcal{SC}}$ securely realizes $\text{IDEAL}_{\mathcal{F}_{\mathcal{SC}}}$.

We have also:

- defined ideal functionalities for secure messaging (\mathcal{F}_{SM}) and for a public key infrastructure (\mathcal{F}_{CA}).

We have also:

- defined ideal functionalities for secure messaging (\mathcal{F}_{SM}) and for a public key infrastructure (\mathcal{F}_{CA}).
- constructed a protocol that realizes \mathcal{F}_{SM} in the $(\mathcal{F}_{CA}, \mathcal{F}_{SC})$ -hybrid model.

Thank you!