Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm

By Mihir Bellare and Chanathip Namprempre

Some slides were also taken from Chanathip Namprempre's defense

DBSEM, May 11, 2004
http://www.ifi.uio.no/dbsem/

Habtamu Abie

Norwegian Computing Center

http://www.nr.no/

Outline

- Introduction
  - Authenticated encryption scheme
  - Relations among notions
  - Analysis of generic composition
- Authenticated Encryption
  - Basic Schemes
  - Generalized Schemes
  - Security of the composite schemes
- Conclusions
- References

Introduction

- Considers two notions of authenticity for symmetric encryption schemes
  - integrity of plaintexts
  - integrity of cipher-texts
- Relates these to the standard notions of privacy for symmetric encryption schemes
  - by implications and separations between all notions
- Analyzes the security of authenticated encryption schemes designed by
  - "generic composition,“ - making black-box use of a given Symmetric Encryption scheme and a given MAC.

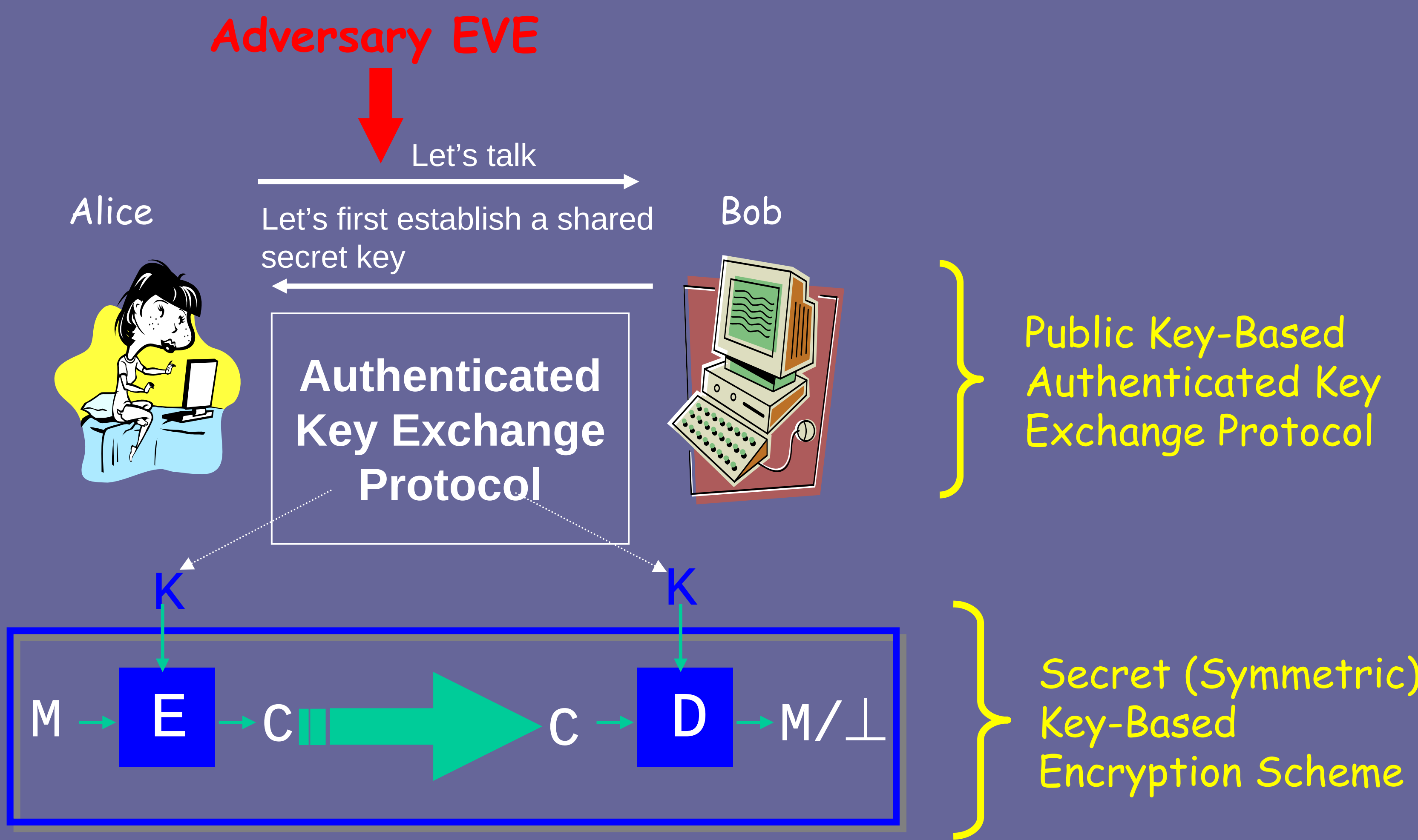
Introduction…

- Authenticated encryption schemes
  - symmetric-key mechanisms by which a message M is transformed into a ciphertext C
  - C protects both **privacy** and **authenticity**

- Tools for achieving Privacy and Authenticity
  - Encryption schemes for privacy
  - Message authentication schemes for authenticity
  - Provable security analyses

- Simultaneously achieving **privacy** and **authenticity** by combining these tools

Symmetric Encryption Setting



Authenticated Encryption Scheme

- Authenticated Key Exchange (KE) Protocol
  - Constructions: Variants of Diffie-Hellman, protocols based on public-key encryption and signature schemes
  - Security Notions: Entity authentication and key exchange
- Symmetric Key-Based Encryption Scheme
  - Constructions: CBC-mode encryption, CTR-mode encryption, OFB mode
  - Security notions: Authenticity and Privacy
    - Authenticity: Integrity of both plaintexts and ciphertexts
    - Privacy: Indistinguishability and Non-malleability under either chosen-plaintext attacks or adaptive chosen-ciphertext attacks
- Relevance to Internet Security
  - Many popular Internet protocols rely on authenticated encryption schemes for privacy and authenticity.
    - Examples: SSL, TLS, SSH, IPSEC, etc.
  - Many applications on the Internet require both privacy and integrity
    - Examples: online banking, retail, and auctions, secure file transfer

Attack Models

- ***Ciphertext-only attack***
  - deduce the decryption key or plaintext by only observing ciphertext
- ***Known plaintext attack***
  - reveal further secret information (typically the secret key) by making use of samples of both plaintext and ciphertext
- ***Chosen plaintext attack***
  - gain further secret information by choosing arbitrary plaintexts to be encrypted and obtaining the corresponding ciphertexts
- **Adaptive chosen-plaintext attack**
  - choose subsequent plaintexts based on the information received from previous requests
- ***Chosen-ciphertext attack***
  - deduce the plaintext from (different) ciphertext by selecting the ciphertext and acquiring the corresponding plaintext
- ***Adaptive chosen-ciphertext attack***
  - choose subsequent ciphertexts based on the information received from previous requests

Privacy: Symmetric Encryption Scheme

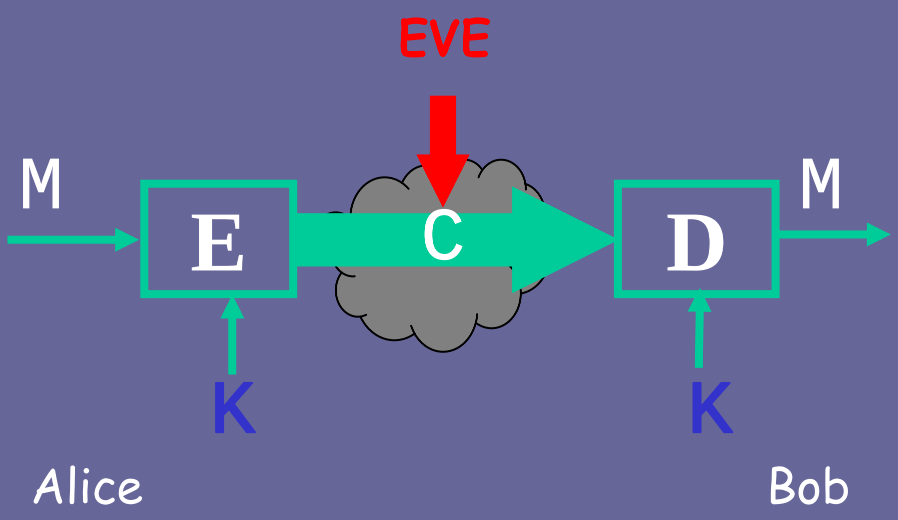
Key ……………. **K**

Message ………. M

Ciphertext ……….C

Encryption Alg ….. **E**

Decryption Alg ….. **D**



Goal: It should be hard for EVE to obtain partial information about M

Thus preventing exposure of transmitted information

Authenticity: Message Authentication Codes (MACs)

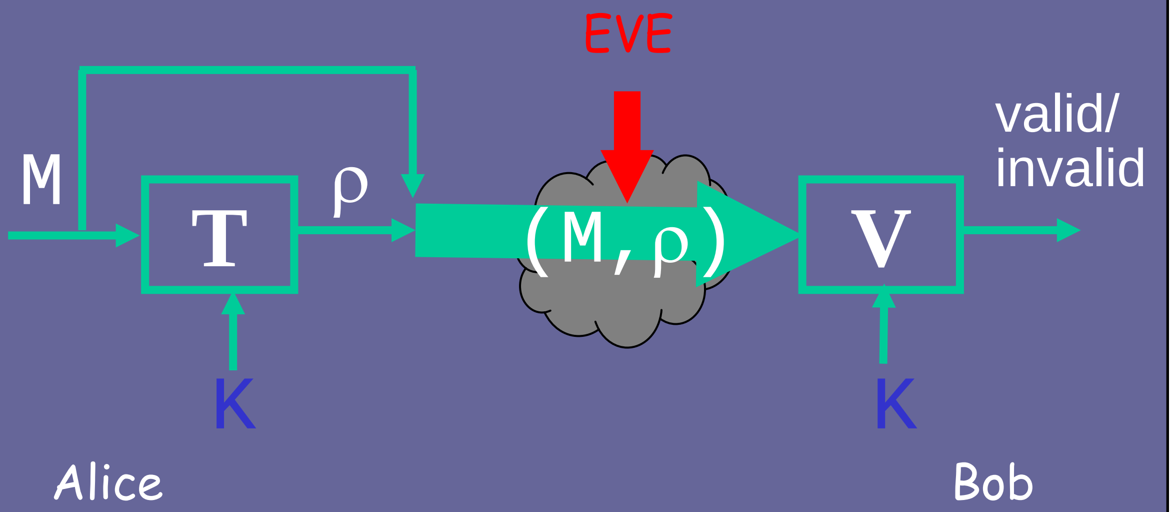
Key …………… K

Message ……… M

Tag ……………..ρ

MAC Alg ……….. **T**

Verification Alg …. **V**



Goal: It should be hard for EVE to forge a valid new pair (M,ρ)

Thus preventing modification of transmitted information

Constructions: CBC MAC, HMAC, UMAC

Privacy and Authenticity: Authenticated Encryption Scheme

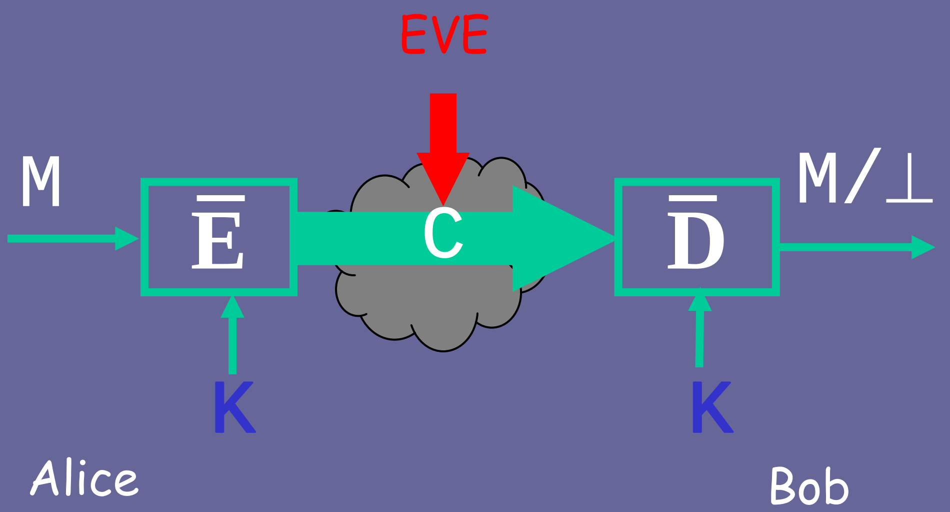
Key …………… **K**

Message ………… M

Ciphertext ……….C

Encryption Alg ….. $\overline{\mathbf{E}}$

Decryption Alg ….. $\overline{\mathbf{D}}$



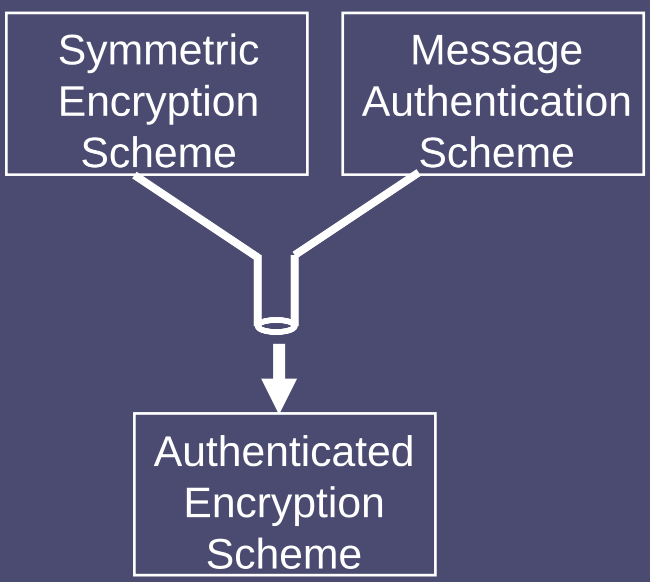
Goal: It should be hard for EVE

- to obtain partial information about M OR
- to forge a valid new ciphertext.

NR

Generic Composition Paradigm

Combine the base schemes as black-boxes



- || denotes appending
- "Decrypt+Verify" process specifies a decryption algorithm $\bar{D}$

Three composition methods are considered

1) Encrypt-and-MAC

$$E_{Ke,Km}(M) = E_{Ke}(M) \,||\, T_{Km}(M)$$

2) MAC-then-Encrypt

$$E_{Ke,Km}(M) = E_{Ke}(M \,||\, T_{Km}(M))$$

3) Encrypt-then-MAC

$$E_{Ke,Km}(M) = E_{Ke}(M) \,||\, T_{Km}(E_{Ke}(M))$$

Generic Composition Results

Composition Method	Privacy			Integrity	
	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-Encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	insecure	insecure	secure	insecure

Under the assumption that the MAC scheme is weakly unforgeable

Composition Method	Privacy			Integrity	
	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-Encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure	secure

Under the assumption that the MAC scheme is strongly unforgeable

Generic Composition Results: Security

Formal security goals for authenticated encryption

- **Authenticity**: Integrity of ciphertexts (INT-CTXT), Integrity of plaintext (INT-PTXT)
- **Privacy**: Indistinguishability and non-malleability each of which can be considered either under chosen-plaintext or (adaptive) chosen-ciphertext attacks (IND-CPA, IND-CCA, NM-CPA, NM-CCA)

Secure: The composite encryption scheme is secure, assuming:

- The component encryption scheme is IND-CPA secure and the base MAC scheme is UF-CMA (Unforgeable under chosen-message attack) secure

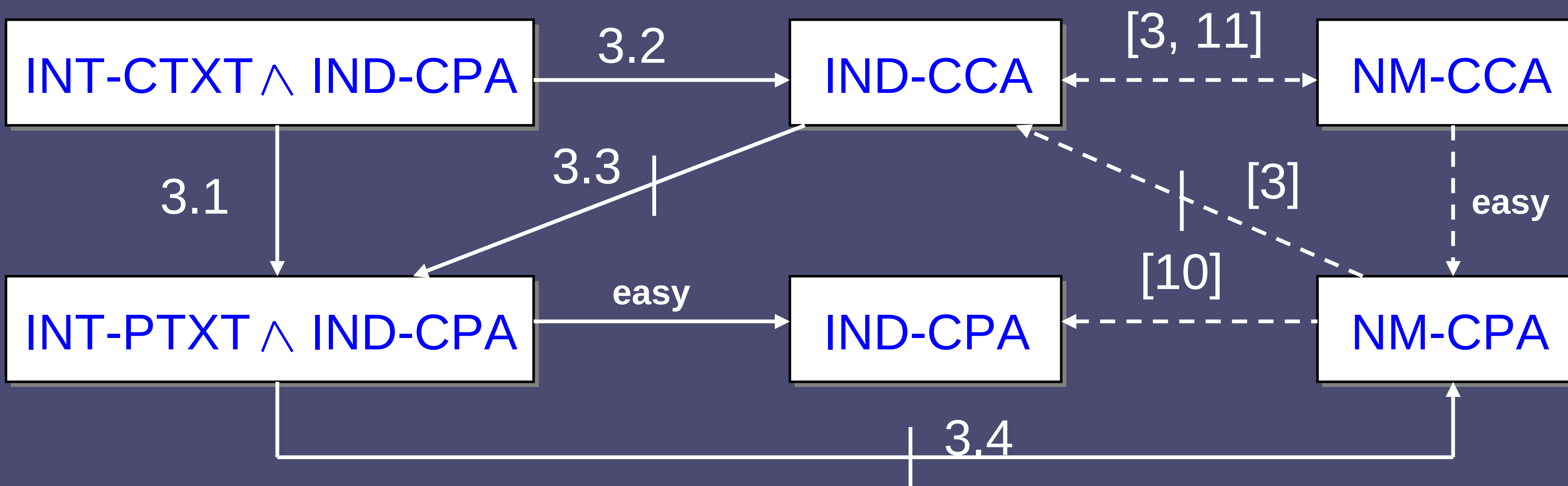
Insecure: The composite scheme is insecure:

- The exists some IND-CPA secure symmetric encryption and some MAC UF-CMA such that the composite scheme based on them does not meet the security requirement in question

Generic Composition Results: Benefits

- Any pseudorandom function is a strongly unforgeable MAC, and most practical MACs seem to be strongly unforgeable.
  - Therefore, analyzing the composition methods under this notion is a realistic and useful approach
- The use of a generic composition method secure in the above sense is advantageous from both performance and of security architecture point of view.
  - The performance benefit arises from the presence of fast MACs such as HMAC and UMAC.
  - The architectural benefits arise from the stringent notion of security being used. To be secure, the composition must be secure for all possible secure instantiations of its constituent primitives. (If it is secure for some instantiations but not others, we declare it insecure.)
  - An application can thus choose a symmetric encryption scheme and a message authentication scheme independently and then appeal to some fixed and standard composition technique to combine them.
  - No tailored security analysis of the composed scheme is required.

Relations among Notions



- INT-PTXT – Integrity of Plaintext
- INT-CTXT – Integrity of Ciphertext
- IND-CPA – Indistinguishability of Chosen-Plaintext Attack
- IND-CCA – Indistinguishability of Chosen-Ciphertext Attack
- NM-CPA – Non-malleability of Chosen-Plaintext Attack
- NM-CCA – Non-malleability of Chosen-Ciphertext Attack

Definition: Indistinguishability of SES

Informally, two different messages cannot be distinguished

Experiment $\mathbf{Exp}^{\text{ind-cpa-}b}_{\mathcal{SE},A_{\text{cpa}}}(k)$

$K \xleftarrow{R} \mathcal{K}(k)$

$x \leftarrow A_{\text{cpa}}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))}(k)$

Return x

Experiment $\mathbf{Exp}^{\text{ind-cca-}b}_{\mathcal{SE},A_{\text{cca}}}(k)$

$K \xleftarrow{R} \mathcal{K}(k)$

$x \leftarrow A_{\text{cca}}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b)),\mathcal{D}_K(\cdot)}(k)$

Return x

Adversary Experiment

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k) = \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1\right]$$

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{SE},A_{\text{cca}}}(k) = \Pr\left[\mathbf{Exp}^{\text{ind-cca-1}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cca-0}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1\right]$$

Adversary Advantages

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) = \max_{A_{\text{cpa}}}\{\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{SE}}(k, t, q_e, q_d, \mu_e, \mu_d) = \max_{A_{\text{cca}}}\{\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{SE},A_{\text{cca}}}(k)\}$$

Adversary Advantage Functions

time-complexity t, E_K(LR(; ; b)) encryption oracle, q_e queries, μ_e bits sum lengths, D_K(.) decryption oracle, q_d queries, μ_e bits sum lengths

Definition: Non-malleability of SES

Informally, given the ciphertext, it must be impossible to generate a different ciphertext such that the respective plaintexts are "meaningfully" related.

Experiment $\mathbf{Exp}^{\text{nm-cpa-}b}_{\mathcal{SE},A_{\text{cpa}}}(k)$ $K \xleftarrow{R} \mathcal{K}(k)$ $(\vec{c}, s) \leftarrow A_{\text{cpa}_1}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b))}(k)$ $\vec{p} \leftarrow \vec{\mathcal{D}}_K(\vec{c})$ $x \leftarrow A_{\text{cpa}_2}(\vec{p}, \vec{c}, s)$ Return x	Experiment $\mathbf{Exp}^{\text{nm-cca-}b}_{\mathcal{SE},A_{\text{cca}}}(k)$ $K \xleftarrow{R} \mathcal{K}(k)$ $(\vec{c}, s) \leftarrow A_{\text{cca}_1}^{\mathcal{E}_K(\mathcal{LR}(\cdot,\cdot,b)),\mathcal{D}_K(\cdot)}(k)$ $\vec{p} \leftarrow \vec{\mathcal{D}}_K(\vec{c})$ $x \leftarrow A_{\text{cca}_2}(\vec{p}, \vec{c}, s)$ Return x

$$\mathbf{Adv}^{\text{nm-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k) = \Pr\left[\mathbf{Exp}^{\text{nm-cpa-1}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{nm-cpa-0}}_{\mathcal{SE},A_{\text{cpa}}}(k) = 1\right]$$

$$\mathbf{Adv}^{\text{nm-cca}}_{\mathcal{SE},A_{\text{cca}}}(k) = \Pr\left[\mathbf{Exp}^{\text{nm-cca-1}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{nm-cca-0}}_{\mathcal{SE},A_{\text{cca}}}(k) = 1\right]$$

$$\mathbf{Adv}^{\text{nm-cpa}}_{\mathcal{SE}}(k, t, q_e, \mu_e) = \max_{A_{\text{cpa}}}\{\mathbf{Adv}^{\text{nm-cpa}}_{\mathcal{SE},A_{\text{cpa}}}(k)\}$$

$$\mathbf{Adv}^{\text{nm-cca}}_{\mathcal{SE}}(k, t, q_e, q_d, \mu_e, \mu_d) = \max_{A_{\text{cca}}}\{\mathbf{Adv}^{\text{nm-cca}}_{\mathcal{SE},A_{\text{cca}}}(k)\}$$

Definition: Integrity of AES

Algorithm $\mathcal{D}^*_K(C)$
    If $\mathcal{D}_K(C)| \neq \perp$, then return 1
        Else return 0.

Experiment $\mathbf{Exp}^{\text{int-ptxt}}_{\mathcal{SE},A_{\text{ptxt}}}(k)$
$K \xleftarrow{R} \mathcal{K}(k)$
If $A^{\mathcal{E}_K(\cdot),\mathcal{D}^*_K(\cdot)}_{\text{ptxt}}(k)$ makes a query C to the oracle $\mathcal{D}^*_K(\cdot)$ such that
- $\mathcal{D}^*_K(C)$ returns 1, and
- $M \stackrel{\text{def}}{=} \mathcal{D}_K(C)$ was never a query to $\mathcal{E}_K(\cdot)$

then return 1 else return 0.

Experiment $\mathbf{Exp}^{\text{int-ctxt}}_{\mathcal{SE},A_{\text{ctxt}}}(k)$
$K \xleftarrow{R} \mathcal{K}(k)$
If $A^{\mathcal{E}_K(\cdot),\mathcal{D}^*_K(\cdot)}_{\text{ctxt}}(k)$ makes a query C to the oracle $\mathcal{D}^*_K(\cdot)$ such that
- $\mathcal{D}^*_K(C)$ returns 1, and
- C was never a response of $\mathcal{E}_K(\cdot)$

then return 1 else return 0.

$$\mathbf{Adv}^{\text{int-ptxt}}_{\mathcal{SE},A_{\text{ptxt}}}(k) = \Pr\left[\mathbf{Exp}^{\text{int-ptxt}}_{\mathcal{SE},A_{\text{ptxt}}}(k) = 1\right]$$
$$\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE},A_{\text{ctxt}}}(k) = \Pr\left[\mathbf{Exp}^{\text{int-ctxt}}_{\mathcal{SE},A_{\text{ctxt}}}(k) = 1\right]$$

$$\mathbf{Adv}^{\text{int-ptxt}}_{\mathcal{SE}}(k,t,q_e,q_d,\mu_e,\mu_d) = \max_{A_{\text{ptxt}}}\{\mathbf{Adv}^{\text{int-ptxt}}_{\mathcal{SE},A_{\text{ptxt}}}(k)\}$$
$$\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE}}(k,t,q_e,q_d,\mu_e,\mu_d) = \max_{A_{\text{ctxt}}}\{\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE},A_{\text{ctxt}}}(k)\}$$

Definition: MAC Scheme Security

Experiment $\mathbf{Exp}^{\mathrm{wuf-cma}}_{\mathcal{MA},F_{\mathrm{w}}}(k)$

$K \stackrel{R}{\leftarrow} \mathcal{K}(k)$

If $F_{\mathrm{w}}^{\mathcal{T}_K(\cdot),\mathcal{V}_K(\cdot,\cdot)}(k)$ makes a query (M,σ) to the oracle $\mathcal{V}_K(\cdot,\cdot)$ such that

- $\mathcal{V}_K(M,\sigma)$ returns 1, and
- M was never queried to the oracle $\mathcal{T}_K(\cdot)$,

`then` return 1 `else` return 0.

Experiment $\mathbf{Exp}^{\mathrm{suf-cma}}_{\mathcal{MA},F_{\mathrm{s}}}(k)$

$K \stackrel{R}{\leftarrow} \mathcal{K}(k)$

If $F_{\mathrm{s}}^{\mathcal{T}_K(\cdot),\mathcal{V}_K(\cdot,\cdot)}(k)$ makes a query (M,σ) to the oracle $\mathcal{V}_K(\cdot,\cdot)$ such that

- $\mathcal{V}_K(M,\sigma)$ returns 1, and
- σ was never returned by the oracle $\mathcal{T}_K(\cdot)$ in response to query M,

`then` return 1 `else` return 0.

We define the *advantages* of the forgers via

$$\begin{aligned}
\mathbf{Adv}^{\text{wuf-cma}}_{\mathcal{MA},F_{\mathrm{w}}}(k) &= \Pr\left[\mathbf{Exp}^{\mathrm{wuf-cma}}_{\mathcal{MA},F_{\mathrm{w}}}(k) = 1\right] \\
\mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA},F_{\mathrm{s}}}(k) &= \Pr\left[\mathbf{Exp}^{\mathrm{suf-cma}}_{\mathcal{MA},F_{\mathrm{s}}}(k) = 1\right]
\end{aligned}$$

We define the *advantage functions of the scheme* as follows. For any integers $t, q_t, q_v, \mu_t, \mu_v$,

$$\begin{aligned}
\mathbf{Adv}^{\text{wuf-cma}}_{\mathcal{MA}}(k,t,q_t,q_v,\mu_t,\mu_v) &= \max_{F_{\mathrm{w}}}\{\mathbf{Adv}^{\text{wuf-cma}}_{\mathcal{MA},F_{\mathrm{w}}}(k)\} \\
\mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA}}(k,t,q_t,q_v,\mu_t,\mu_v) &= \max_{F_{\mathrm{s}}}\{\mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA},F_{\mathrm{s}}}(k)\}
\end{aligned}$$

MAC: Theorem: SUF-CMA → WUF-CMA

$$\mathbf{Adv}^{\text{wuf-cma}}_{\mathcal{MA}}(k, t, q_t, q_v, \mu_t, \mu_v) \leq \mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA}}(k, t, q_t, q_v, \mu_t, \mu_v)$$

Proof: A tag corresponding to new message is clearly a new tag for that message

$$\mathbf{Adv}^{\text{wuf-cma}}_{\mathcal{MA},F_{\text{w}}}(k) \leq \mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA},F_{\text{s}}}(k)$$

Associate Fw with WUF-CMA and Fs with SUF-CMA

Fs uses the same amount of resources as Fw does.

Set Fs to be exactly the same as Fw. Then, the theorem follows

Relations among Notions of Symmetric Encryption

Theorem 3.1 (INT-CTXT → INT-PTXT)

$$\mathbf{Adv}^{\text{int-ptxt}}_{\mathcal{SE}}(k, t, q_e, q_d, \mu_e, \mu_d) \leq \mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE}}(k, t, q_e, q_d, \mu_e, \mu_d)$$

Proof: This is true because an adversary that violates integrity of plaintexts of a scheme *SE = (K, E,D)* also violates integrity of ciphertexts of the same scheme

$$\mathbf{Adv}^{\text{int-ptxt}}_{\mathcal{SE},A}(k) \leq \mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE},A'}(k)$$

Let C be winning query made by A to $D^*_k(.)$ such that it returns 1 but

$$M \stackrel{\text{def}}{=} \mathcal{D}_K(C)$$

was never queried to the $E_k(.)$

A uses the same amount of resources as A' does.
Set A' to be exactly the same as A. Then, the theorem follows

Encrypt-then-MAC

$SE = (K_e, E, D)$ a symmetric encryption scheme

$MA = (K_m, T, V)$ a MAC scheme

$\overline{SE} = (\overline{K}, \overline{E}, \overline{D})$ a composite scheme

The composite scheme is defined as follows:

Algorithm $\overline{\mathcal{K}}(k)$ $K_e \stackrel{R}{\leftarrow} \mathcal{K}_e(k)$ $K_m \stackrel{R}{\leftarrow} \mathcal{K}_m(k)$ Return $\langle K_e, K_m \rangle$	Algorithm $\overline{\mathcal{E}}_{\langle K_e, K_m \rangle}(M)$ $C' \leftarrow \mathcal{E}_{K_e}(M)$ $\tau' \leftarrow \mathcal{T}_{K_m}(C')$ $C \leftarrow C' \\| \tau'$ Return C	Algorithm $\overline{\mathcal{D}}_{\langle K_e, K_m \rangle}(C)$ Parse C as $C' \\| \tau'$ $M \leftarrow \mathcal{D}_{K_e}(C')$ $v \leftarrow \mathcal{V}_{K_m}(C', \tau')$ If $v = 1$, return M else return $\perp$.

Encrypt-then-MAC

Security		Weak MAC		Strong MAC	
		Result	Reason	Result	Reason
Privacy	IND-CPA	Secure	Theorem 4.7	Secure	Theorem 4.9
	IND-CCA	Insecure	NM-CPA insecure and NM-CPA $\rightarrow$ IND-CCA	Secure	Theorem 4.9
	NM-CPA	Insecure	Proposition 4.6	Secure	IND-CCA secure and IND-CCA $\rightarrow$ NM-CPA
Integrity	INT-PTXT	Secure	Theorem 4.7	Secure	INT-CTXT secure and INT-CTXT $\rightarrow$ INT-PTXT
	INT-CTXT	Insecure	IND-CPA secure and NM-CPA insecure and INT-CTXT$\wedge$IND-CPA $\rightarrow$ NM-CPA	Secure	Theorem 4.9

Summary of results for the Encrypt-then-MAC composition method

Meadows' Classification of Analysis Techniques

- **Type I**
  - models and verifies protocols using specification languages and verification tools not specifically developed for the analysis of cryptographic protocols, e.g., CSP and FDR
- **Type II**
  - uses expert systems to create and examine different scenarios that enable protocol designers to draw conclusions about the security of the protocols being studied, e.g., ProtSpec (Snekkenes') HOL based system
- **Type III**
  - models requirements of a protocol family using logics developed specifically for the analysis of knowledge and belief, e.g., BAN
- **Type IV**
  - develops a formal model based on the algebraic term-rewriting properties of cryptographic systems (Can an initial state lead to an undesirable state?), e.g., NRL (Naval Research Lab) Protocol Analyzer
- **Type V (an extension by a master student)**
  - proves security via a complexity-theoretic approach, e.g., Bellare-Rogaway

Conclusions

- Join in recommending: Use Encrypt-then-MAC

And

Thanks for your attention !

References

- M. Bellare and C. Namprempre, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”, Asiacrypt 2000.
  - http://www-cse.ucsd.edu/users/mihir/papers/oem.pdf
- Chanathip Namprempre's Home page
  - http://www.cs.ucsd.edu/~cnamprem/
- Peter Guttman's tutorial: about 500 slides covering cryptography, secure connection protocols, PKI, politics and what have you
  - http://www.cs.auckland.ac.nz/~pgut001/tutorial/
- Modes of Operation for Symmetric Block Ciphers and for authenticated Encryption
  - http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/