Hybrid Signcryption with Outsider Security

Alexander W. Dent

ROYAL HOLLOWAY, UNIVERSITY OF LONDON
Information Security Group

Signcryption

- Introduced by Zheng 1997.
- Combines advantages of PKE and signatures:
  - Confidentiality
  - Integrity/Origin authentication
  - Non-repudiation?
- A relatively new type of primitive.
- We haven't even agreed a security model yet.

Signcryption

- A common parameter generation algorithm.
- A receiver key-pair (pk_R,sk_R) generation algorithm.
- A sender key-pair (pk_S,sk_S) generation algorithm.
- A generation-encryption algorithm.
- A verification-decryption algorithm.

Signcryption

- An, Dodis and Rabin (2002) security model.
- This is a two user model.
- Outsider security
  - Security against all third parties, i.e. anyone who isn't the sender or receiver.
- Insider security
  - Full security, including integrity protection against attacks made by the receiver.
- Baek, Steinfeld and Zheng (2002) model.

Signcryption: confidentiality

- No third party can distinguish between a signcryption of one message and a signcryption of another message.
- Normal IND criteria, except that we must provide the attacker with encryption and decryption oracles.
- We do not consider forward security (with can be expressed using the Baek *et al.* model).

Signcryption: integrity

- An outside attack is one in which a third party attempts to forge a signcryption from the sender to the receiver.
- Normal existential unforgeability game, except that the attacker has access to encryption and decryption oracles.
- It has a similar security guarantee to a MAC.
- This is satisfactory for most applications (but gives simpler schemes).

Signcryption: non-repudiation

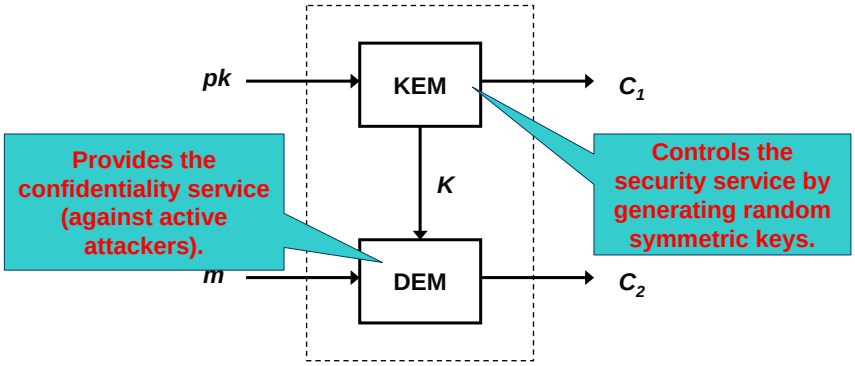
- The ability for a third party to check that a given signcryption is a proper signcryption of a given message.
- Not required for most applications.
- Schemes which are outsider secure can never provide non-repudiation.
- Most signcryption schemes “cheat” and use NIZK proofs.

Hybrid encryption

- Involves the use of black-box symmetric algorithms with certain security properties.
- Very popular trick:
  - ECIES/DHAES
  - Fujisaki-Okamoto and related transforms.
- Most use the same “trick” of encrypting a random symmetric key with the asymmetric algorithm.
- Formalised by Cramer and Shoup (2004).

ROYAL HOLLOWAY, UNIVERSITY OF LONDON
Information Security Group

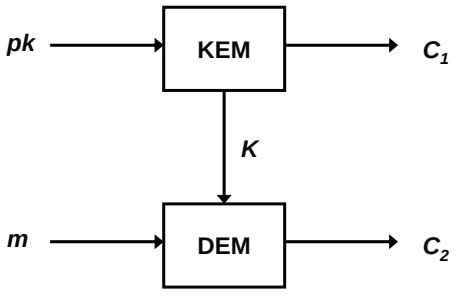
Hybrid encryption



9

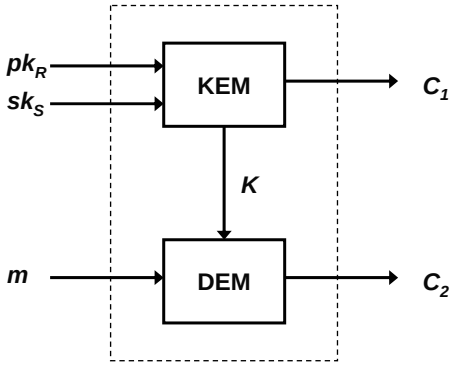
ROYAL HOLLOWAY, UNIVERSITY OF LONDON
Information Security Group

Hybrid signcryption



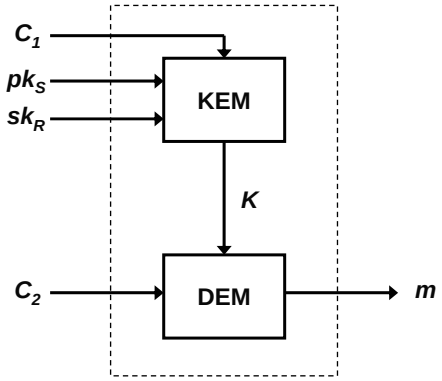
10

Hybrid signcryption

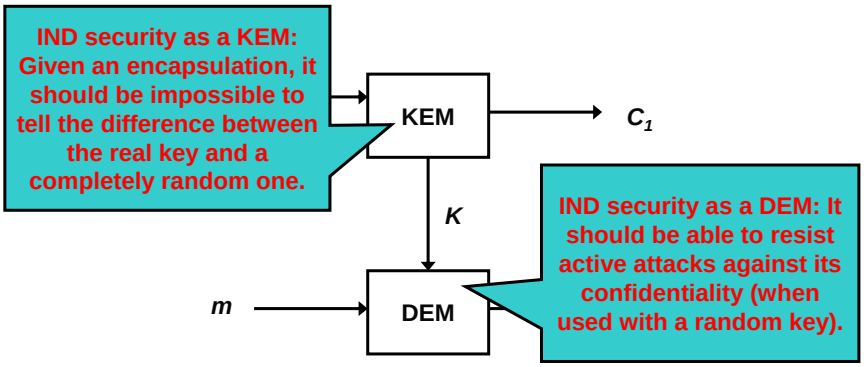


ROYAL HOLLOWAY, UNIVERSITY OF LONDON
Information Security Group

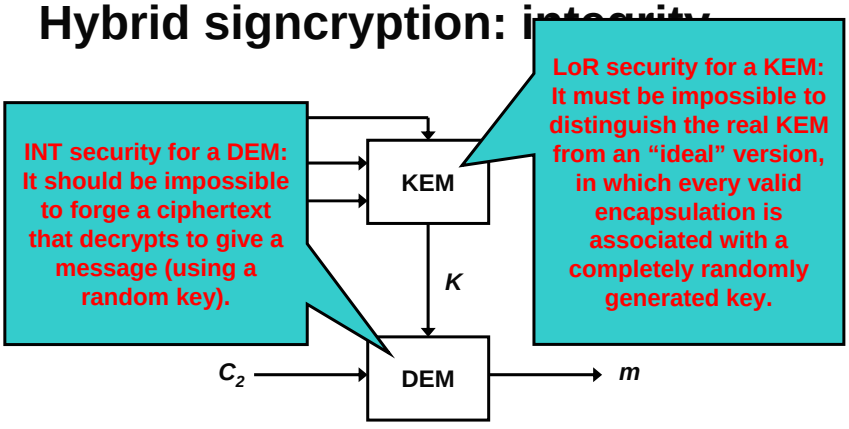
Hybrid signcryption



Hybrid signcryption: confidentiality



Hybrid signcryption: integrity

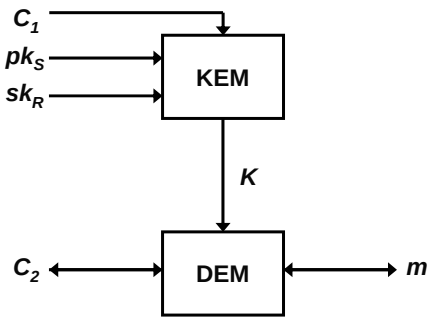


All practical (encryption) DEMs are INT and IND secure!

Hybrid signcryption

- Very easy to "bolt on" outsider secure hybrid signcryption to hybrid encryption schemes.
- The paper contains a practical signcryption KEM which we call ECISS-KEM:
  - Encryption: One exponentiation (and one pre-computed group exponentiation).
  - Decryption: One group multiplication (and one pre-computed group exponentiation).

Hybrid signcryption



- The attacker finds a valid signcryption (C_1,C_2).
- Recovers the key K associated with C_1.
- Computes C_2'=DEM$_K$(m').
- (C_1,C_2') is a forgery.

Hybrid signcryption

There must be a binding between the message *m*, the encapsulation C_1 and the symmetric key *K*.

Key agreement using KEMs

- KEMs and key agreement mechanisms have a lot in common...
- ...but KEMs can only be thought of as the most basic method of agreeing a key.
- No authentication or freshness guarantees.
- Signcryption KEMs go part of the way to solving this problem by allowing the users to authenticate each other.

Key agreement using KEMs

- Alice uses a signcryption KEM to compute a (K,C) pair.
- Use the key K to compute the MAC of a timestamp t.
- Sends (C,t,MAC) to Bob.
- Bob checks the timestamp t is current.
- Recovers the key K using the signcryption KEM.
- Checks the authenticity of the MAC on the timestamp.

Vulnerable to a known-key attack!

Insider security

- A paper appeared in ACISP 2005 describing a construction paradigm for a hybrid signcryption scheme with insider security.
- A paper is currently being prepared which improves on this result using tag-KEMs.
- This also allows us to build key agreement mechanisms.

Open problems

- Can we use this framework to develop new schemes?

Open problems

- No satisfactory model for multi-user security.
- Multi-user model should allow the attacker to initiate users, replace public keys?, corrupt users, make test queries, force users to encrypt messages, force users to decrypt signcryptions.
- Similar to Certificateless PKE security model.
- Should be easy for outsider security!

Conclusions

- Signcryption schemes are easy to build if we recognise that outsider security is all that is required for a lot of applications.
- It's easy to build efficient, provably secure hybrid signcryption schemes.
- However, more work can be done in this particularly under-researched area.