Hybrid Signcryption with Insider Security

Alexander W. Dent

Signcryption

- 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

- 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.
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 (which can be expressed using the Baek et al. model).

Signcryption: integrity

- Attacker in possession of the receiver’s private key must attempt to forge a signcryption from the sender.
- Normal existential unforgeability game.
- Attacker has access to an encryption oracle for the sender.
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.
- Most signcryption schemes “cheat” and use NIZK proofs.
- A trend that we will continue.

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.
Hybrid encryption

Hybrid signcryption
Hybrid signcryption

The attacker finds a valid signcryption \((C_1, C_2)\). They recover the key \(K\) associated with \(C_1\). They compute \(C_2' = \text{DEM}_K(m')\). \((C_1, C_2)\) is a forgery.

There must be a binding between the message \(m\), the encapsulation \(C_1\) and the symmetric key \(K\).
Hybrid signcryption

\[ \begin{align*}
 p_{KR} & \quad \text{KEM} \quad C_1 \\
 sk_S & \quad K \\
 m & \quad \text{DEM} \quad C_2
\end{align*} \]
Hybrid signcryption

Note that the KEM necessarily provides a signature on the message, where

- The signing algorithm is given by KEM.
- The verification algorithm is given by VER.

Therefore, the KEM provides the integrity service...

...and the DEM only has to provide a confidentiality service.

Arguably closer to Fujisaki-Okamoto than Cramer-Shoup.
Hybrid signcryption: confidentiality

The KEM must be INP secure, i.e. it must be impossible to tell which message an encapsulation is associated with.

Since the KEM is providing integrity protection, the DEM only needs to be passively secure.

The DEM must be IND secure, i.e. it must be impossible to tell which message a ciphertext is an encryption of.

The KEM must be IND secure, i.e. produces keys that look random to the attacker.

Hybrid signcryption: integrity

Must be existentially unforgeable, i.e. it must be impossible for any attacker to find a message/encapsulation pair that the VER algorithm accepts as valid.
Hybrid signcryption

- Need to present a scheme to demonstrate practicality of this construction paradigm.
- Many schemes already exist in the literature.
- In particular, the Baek et al. variant of Zheng’s original signcryption scheme is provably secure as a hybrid signcryption scheme.
- Note that efficiency can be gained by re-using in the VER variables calculated in the KEM.

Open problems

- Can we use this framework to prove the security of previously unproven schemes?
- Can we use this framework to develop new schemes?

- Schemes with better non-repudiation properties?
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 signcryption.
- Similar to Certificateless PKE security model.
- Should be easy for outsider security!

Open problems

- Implicit link between the message (in the form of the DEM encryption $C_2$) and the symmetric key used to encrypt it!
- Great potential for more efficient insider secure hybrid signcryption schemes.

Conclusions

- Signcryption schemes can be built using a hybrid approach, separating the scheme into independent building blocks.
- Most known schemes have implicitly used this construction.
- However, more work can be done in this particularly under-researched area.