

Certificateless Cryptography II

Kenny Paterson

Information Security Group

Royal Holloway, University of London

`kenny.paterson@rhul.ac.uk`

June 2007

Recapitulation

- Certificateless cryptography seems to be an interesting alternative to PKI/ID-PKC.
- User supplies portion of private key; KGC supplies portion of private key.
- Need to model attackers who can replace public keys and/or who know master secret.
- Specific and generic constructions for CLE schemes meeting strong security notions known in ROM and standard model.

Overview

- CLE and Certificate-Based Encryption
- Denial-of-Decryption Attacks and Malicious KGCs
- Mediated certificateless encryption, certificateless signatures (CLS) and further certificateless primitives
- Conclusions and open problems

1 Certificate-Based Encryption (CBE)

Gentry's CBE concept (2003) simplifies revocation in traditional PKIs.

- User selects key-pair $\langle sk, pk \rangle$.
- Certificate $\text{Cert}_\tau(pk)$ is pushed to user at regular time intervals by CA.
- Encrypting party uses only CA parameters, pk and current time τ to encrypt to user.
- User needs private key sk and current certificate $\text{Cert}_\tau(pk)$ to be able to decrypt.
- CA simply omits to push new certificates to revoked users.

CLE and CBE

CBE and CLE concepts independently developed, yet closely related.

- Full private keys formed by combining TTP-supplied component with user-generated component in both approaches.
- Implicit security in both approaches: legitimate user can only decrypt if in possession of both private components.
- Certificates in CBE resemble partial private keys in CLE.
- CBE adversary gets to see all certificates; CLE adversary could query for all partial private keys.

What is the exact nature of the relationship between CBE and CLE?

CLE and CBE

Al-Riyami–Paterson (2005):

- Slight reformulation of CBE concept to clarify and correct minor problems with original CBE definitions.
- Modification of Type II (insider) security model for CBE:
 - Adversary is given CA parameters instead of choosing them for himself;
 - Adversary can select any one of several public keys for challenge instead of being given single public key.

CLE and CBE

Al-Riyami–Paterson (2005):

- Generic conversion from a CL-PKE scheme to a CBE scheme (but not vice-versa!)
- Conversion is security preserving for Type I attackers.
- Same claim made for Type II attackers, but unproven.
 - Shown by Kang-Park (2005) that proof technique used for Type I attackers is unlikely to extend to Type II case.

Exact relationship between CBE and CLE still remains somewhat unclear.

2 Pairing-free CLE and Denial-of-Decryption

- Up to this point, all CLE constructions have used pairings.
- Pairings can be avoided using, e.g., Cocks' IBE combined with Libert-Quisquater generic conversion, but schemes are rather inefficient.

In fact, since CLE implies IBE, we cannot hope for an efficient pairing-free CLE scheme until we have the equivalent for IBE.

Pairing-free CLE?

Baek *et al.* (2005):

- Gave an efficient, pairing-free construction for CLE, but scheme does not strictly conform to the Al-Riyami–Paterson model.
- It requires that the partial private key be generated prior to the public key.
- In other words, d_{ID} is an additional input to **Set-Public-Key**.
- This decreases flexibility of CLE and, in particular, rules out attractive work-flow applications.
- Flaw in proof announced by Baek (2007).

Denial-of-Decryption Attacks

DoD concept introduced by Liu-Au-Susilo (2007):

- No certificates to allow sender to select the true public key.
- What if sender faced with a choice of public keys, or the wrong public key?
- Attacker could mount “Denial-of-Decryption” (DoD) attack:
 - Public key replacement by adversary tricks sender into using *wrong* public key.
 - Thus denying recipient opportunity to decrypt.
 - Or resulting in a wrong plaintext upon decryption.

Denial-of-Decryption Attacks

- Such attacks are endemic in the usual CLE setting, since adversary can always run `Set-Secret-Value` then `Set-Public-Key` to produce a valid public key.
- Is such a Denial-of-Service attack actually within the proper domain of cryptography?
- If we accept that it is, can a DoD attack be prevented?
- Perhaps if `Set-Public-Key` involves partial private key as input (c.f. idea of Baek *et al.*), thus preventing adversary from generating valid public keys.
- But then workflow cannot be achieved if DoD attacks are to be prevented.

Modeling Denial-of-Decryption Attacks

- Challenger runs Setup for CLE scheme to create $\langle msk, mpk \rangle$.
- Adversary \mathcal{A} has access to usual oracles.
- \mathcal{A} wins if he can create a public key pk_{ID^*} for the challenge identity ID^* and a challenge message m^* such that:
 - Encrypt run on input $\langle mpk, ID^*, pk_{ID^*}, m^* \rangle$ produces a valid ciphertext C^* (not \perp); and
 - Decrypt run on sk_{ID^*} and C^* produces \perp or a message $m' \neq m^*$.
- Here, the private key used to decrypt is the *original* private key held by the user.

Modeling Denial-of-Decryption Attacks

- Only restriction on oracle access: \mathcal{A} may not query partial private key extract oracle on ID^* (otherwise \mathcal{A} can trivially win game).
- DoD adversary has access to a weak Type Ia decryption oracle
- A CLE scheme is said to be DoD-Free if no polynomial-time attacker \mathcal{A} has non-negligible success probability in the above game.

DoD-Free CLE

Liu *et al.* (2007) generic construction for DoD-Free CLE:

- Combination of CLE and certificateless signature scheme (CLS).
- Two partial private keys, one for CLE, the other for CLS.
- Single public key pk and single secret value x .
- Two full private keys – one for CLE, one for CLS.
- User signs his public key pk using CLS private key to obtain σ .
- User's final public key is $\langle pk, \sigma \rangle$.
- Sender checks CLS signature σ in public key before encrypting using CLE scheme.
- Recipient uses CLE private key to decrypt.

DoD-Free CLE

- General approach is called *self-generated certificate PKC* (SGC-PKC) by Liu *et al.*
- Somewhat analogous to self-signed certificates in PKI.
- Generic construction can be instantiated with standard model CL components to obtain weak Type Ia DoD-Free security in the standard model.

DoD – A Thought Experiment

- DoD approach requires the user to interact with KGC *before* his public key can be finalised.
- So why not allow the user to run an interactive protocol with the KGC in which the KGC signs the user's public key pk , instead of the user signing with KGC-issued partial private key?
 - So KGC supplies a certificate Cert to the user.
 - Replace $\langle pk, \sigma \rangle$ with $\langle pk, \text{Cert} \rangle$.
 - Sender still checks signature Cert in public key before encrypting using CLE scheme.
- Isn't this rather familiar?

3 Malicious KGCs in Certificateless Cryptography

- So far we have assumed an honest-but-curious KGC.
- What if we have a nastier KGC?
- KGC could choose mpk in an adversarial way, or issue special partial private keys d_{ID} , with the intention of later being able to decrypt ciphertexts.
- CBE paper of Gentry already covers this to some extent.
 - Type II attacker in CBE model chooses mpk in Gentry's original model.
 - Weakened in Al-Riyami–Paterson reformulation of CBE!

Malicious KGCs in Certificateless Cryptography

- Au et al. (2007) formalised concept of malicious KGC attacks and found attacks on various schemes:
 - Al-Riyami–Paterson (2003) scheme: KGC can learn private key for a single, pre-selected identity.
- Attacks on several other CLE (and CLS) schemes were then forthcoming.
- Huang-Wong (2007): malicious KGC attack against the Liu-Au-Susilo DoD-Free CLE scheme in which adversary can decrypt ciphertexts intended for *any* entity.
- Similar attack also possible against the standard model secure CLE scheme of Dent-Libert-Paterson.

Malicious KGCs in Certificateless Cryptography

Au *et al.* (2007) also established the security of CLE (and CLS) schemes against malicious KGC attacks in an appropriate security model:

- IND-CPA-security against malicious KGCs for “PKE followed by IBE” generic construction.
- IND-CCA-security against malicious KGCs for Libert-Quisquater FO-style conversion applied to the above generic construction.
- Model allows strong Type I and II decrypt queries.

Malicious KGCs in Certificateless Cryptography

Huang-Wong (2007):

- IND-CCA-security against malicious KGCs for “IBE followed by PKE” construction, augmented with one-time signature/one-time MAC.
- Similar to Dodis-Katz construction for two-key PKE.
- Idea is that outer encryption cannot be undone by KGC, no matter what nasty IBE scheme he creates.
- Allows standard model security using right components.
- But security model weakened to equivalent of Weak Type Ib/Iib for decryption queries: use original private key to decrypt if public key replaced.

Malicious KGCs in Certificateless Cryptography

Is it possible to have strong Type I/II decrypt queries and security against malicious KGCs?

- Yes, in the ROM (Au *et al.*)
- Not known in standard model.
- Standard model simulation used to handle Type I attacker could be used to build malicious Type II attacker?

4 Security Mediated Certificateless Encryption

What if instant revocation of security capabilities is needed?

For example, in high-security or business-critical applications, it may be desirable to dynamically control use of private keys of users.

Mediated cryptography concept of Boneh *et al.*:

- Add a *security mediator* (SEM) – an on-line semi-trusted party that needs to be involved in every decryption/signing operation.
- SEM can make policy-based decisions on whether to allow decryption to proceed or not.
- Ding-Tsudik (2003): SEM in the ID-PKC setting.

Security Mediated Certificateless Encryption

Chow–Boyd–González-Nieto (2006):

- Add instant revocation to CLE by introducing a SEM.
- Natural development of mediated cryptography concept of Boneh *et al.*
- Focus on encryption capability, giving formal definition of security for SEM-CLE.
- Generic construction based on Dodis-Katz multiple encryption, combining PKE scheme (user controlled), IBE scheme (with private keys given to SEM) and one-time signature.
- Similar approach to Huang-Wong construction for CLE secure against malicious KGC, but for different purpose.

5 Certificateless Signatures (CLS)

We have already mentioned CLS several times.

In general, a CLS scheme is defined by 7 algorithms:

Setup, Extract-Partial-Private-Key, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Sign, and Verify.

First five function just as in CLE, and:

Sign:

- Input: mpk , sk_{ID} , and message M .
- Output: signature σ .

Verify:

- Input: mpk , ID , pk_{ID} , message M , and string σ .
- Output: valid or invalid.

Certificateless Signatures

- Obvious correctness requirement:

$$\text{Verify}(mpk, ID, pk_{ID}, M, \text{Sign}(mpk, sk_{ID}, M)) = \text{valid}.$$

i.e. running `Verify` on an output of the `Sign` algorithm will lead to `valid` as output.

- 5 algorithm formulation for CLS also possible.
- Type I and II adversaries roughly as in CLE.

Certificateless Signatures

- A CLS scheme was sketched by Al-Riyami and Paterson (2003), without formal security model or security analysis.
- Subsequently shown by Huang *et al.* (2005) to be insecure under Type I public key replacement attack (without using signing oracle).
- Huang *et al.* also provided a security model for CLS, and a provable fix to the Al-Riyami–Paterson scheme.
- Security model allows signature queries for replaced public keys, but only if new secret value supplied.
 - Analogous to Weak Type Ia model in CLE setting.

Certificateless Signatures

- Zhang *et al.* (2006): “new” security model for CLS, but hard to distinguish from model of Huang *et al.*:
 - Signing queries are answered using old private key or maybe new private key if new secret value supplied by adversary.
- Proof for concrete scheme seems to allow analogy of Strong Type I CLE decryption queries:
 - Challenger correctly responds to signing queries for replaced public keys (i.e. responses verify correctly with new public key), even when new secret values not supplied.
 - So model used in proof seems to be stronger than model given in paper!
- Signatures consist of 2 group elements; signing is pairing-free, verification needs 4 pairings.

Certificateless Signatures

- Yum-Lee (2004) proposed a generic construction for CLS using IBS and standard PKS – essentially, iterated signing.
- Hu *et al.* (2006a) showed that the Yum-Lee construction can not be generically secure under key replacement attacks.
 - There exist specific secure components leading to an insecure CLS scheme.
 - Attack exploits fact that for some standard PKS, it is possible to find two message/public key pairs resulting in the same signature.

Certificateless Signatures

Hu *et al.* (2006) also gave a 5 algorithm definition for CLS, a variant security model, and a new generic construction.

- Security model requires Type I adversary to supply *some* secret value as part of public key replace queries.
- But it need not be correct secret value!
- And signing queries are answered using whatever value was supplied.
- This appears to be a retrograde step in terms of security modelling.

Certificateless Signatures

Liu-Au-Susilo (2007):

- Construction for CLS in the standard model, using simple variant of the IBS of Paterson-Schuldt (itself a trivial variant of 2-level Waters IBE).
- Security proved in an analogue of Strong Type I CLE security model.
 - Type I adversary can access signing oracle for replaced public keys; output must be valid.
- Scheme is reasonably efficient but has rather large public parameters.

Certificateless Signatures

- There has been a flood of CLS models, concrete proposals, and attacks.
- The flow continues unabated (short CLS signatures, CLS with additional properties, malicious KGC attacks, ...).
- But reasonably efficient, secure IBS schemes can be obtained by using normal PKS twice in a generic construction.
- This exploits fact that signature can “carry” public keys, certificates, etc.
- This applies to CLS as much as it does to IBS!

Generic Certificateless Signatures

- CLS can be built from IBS and PKS (Hu *et al.*, 2006).
- IBS can be built from PKS and PKS (folklore).
- So CLS can be built from PKS, PKS and PKS.
- Can these signatures be aggregated to produce short signatures, if PKS scheme is, say, BGLS?
- Sequential aggregation may be sufficient, in which case short CLS in the standard model may be achievable.
- Do we really need 3 signatures, or would 2 actually suffice (as in IBS)?
- Can we get Strong Type I security?

Why Certificateless Signatures?

- A user needs to interact with KGC to get his partial private key before he can sign in a CLS scheme.
- For signatures, we can always bundle certificates, public keys, etc into the signature.
- So we could replace CLS with a standard PKI signature, with KGC issuing certificate instead of partial private key.
- Why do we need certificateless signatures?
- Benefit seems to be that partial private key does not need to be bound to secret value/public key.
- Are there any good applications for this property?

6 Further Certificateless Primitives

- Hierarchical CLE and CLS sketched in Al-Riyami–Paterson (2003), but no formal security models or proofs.
- Likewise for key exchange.
- Li-Chen-Sun (2005): Proxy CLS.
- Huang *et al.* (2006): Certificateless designated verifier signatures.
- Wang-Zhang (2007): Key agreement for SIP using CL-PKC.
- Chow-Yap (2007): Certificateless ring signatures.
- Wang *et al.* (2007): Certificateless threshold signatures.
- Cao *et al.* (2007): Certificateless group key exchange.
- Yap *et al.* (2007): Security mediated certificateless signatures.

7 Questions and Conclusions

Certificateless cryptography appears to have some attractive properties intermediate between ID-PKC and traditional PKI.

- What is the right security model for CLE and other certificateless primitives?
- What other certificateless primitives are worthy of exploration?
- What is certificateless cryptography good for?
- What practical issues must be addressed in deploying certificateless cryptography?

The last two questions are perhaps now more important than the first two.

Acknowledgements

My thanks to:

- All the staff at ISI, QUT for their generous hospitality.
- Alex Dent for his excellent article “A Survey of Certificateless Encryption Schemes and Security Models”.
- And finally... to Sattam Al-Riyami for asking the initial question that led us to certificateless cryptography.