Formal Proofs for the Security of Signcryption

Joonsang Baek and Ron Steinfeld
School of Network Computing,
Monash University, Australia

Yuliang Zheng
Dept. Software and Info. Systems
UNC Charlotte, USA
Feb. 2002

1

Signcryption

- Proposed by Zheng at Crypto '97
- Provides both message confidentiality and authenticity (non-repudiation & unforgeability) *in an efficient way*
- Has received a lot of attention
  - a number of papers about signcryption have been published
  - Submitted to standard committee P1363

2

Security of signcryption

- However, *formal proofs* for the security of signcryption have not been provided
- Formal proofs
  - "formal proofs" = "reductions from attacking the signcryption scheme to solving computationally difficult problems"
  - To provide formal proofs of security, first of all we need to establish a *sound security model for signcryption*

3

What we have achieved

- A sound security model for signcryption:
  - ***Flexible public key model***
    - encompassing CCA security (security against adaptive chosen ciphertext attack)
  - Attackers in our model are allowed to be very powerful!

4

What we have achieved (cont.)

- Proofs for the confidentiality and unforgeability of signcryption
  - Confidentiality --- Providing a reduction
    - from breaking CCA security of signcryption with respect to the flexible public key model
    - to breaking the ***GAP Diffie-Hellman assumption*** in the ROM (Random Oracle Model)
  - Unforgeability --- Providing a reduction
    - from breaking unforgeability of signcryption against CMA (Chosen Message Attack)
    - to Discrete Logarithm problem in the ROM

5

Difference between our model and previous models

- Motivation
  - An attacker can produce her own public key and replace Alice and/or Bob's public keys to break the confidentiality or authenticity
  - Therefore, the security model of encryption + authentication in asymmetric setting should be different from that in the symmetric setting

6

Difference between our model and previous models (cont.)

- Security model for encryption + authentication (E+A) in the symmetric setting
  - Formalized by Bellare & Namprepre at Asiacrypt 2000 [BN]
  - Only Encryption-then-MAC (EtM) composition is CCA-secure

7

Difference between our model and previous models (cont.)

- Observation:
  - Results on confidentiality in the symmetric setting are NOT applicable to E+A in the asymmetric setting.
  - Specifically, Encrypt-then-Sign (EtS, the corresponding *simple* asymmetric version) *is completely insecure against CCA!*

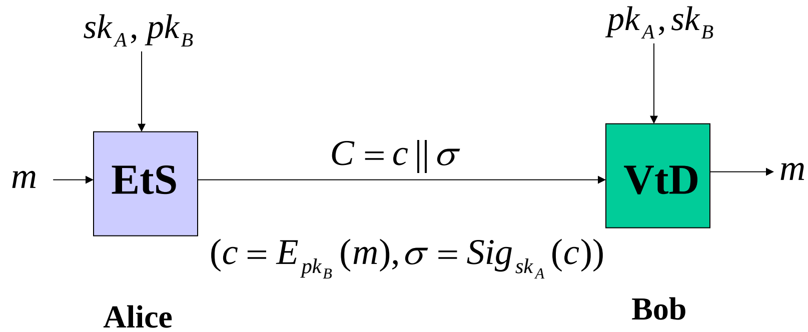
8

CCA attack on the simple EtS

- Simple EtS

Alice's private/public key : (sk_A, pk_A)

Bob's private/public key: (sk_B, pk_B)



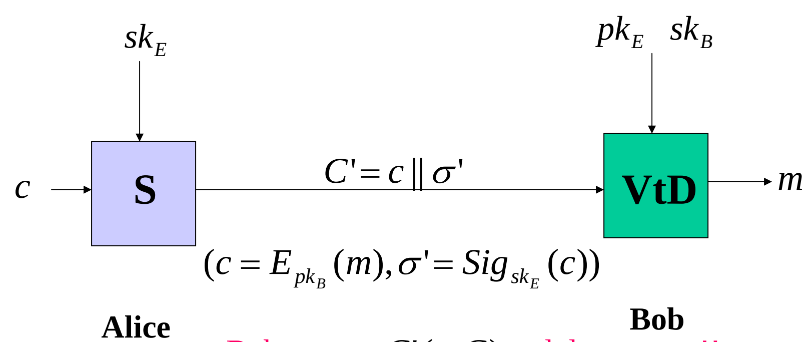
9

CCA attack on the simple EtS

- Attack

Eve's private/public key: (sk_E, pk_E)

Bob's private/public key: (sk_B, pk_B)



Bob accepts $C'(\neq C)$ and decrypts c !!

10

Signcryption: an EaS variant

- Signcryption may be viewed as a variant of the simple EaS (Encrypt-and-Sign) composition.
  - It employs 'EaS' concept to gain efficiency
- However, signcryption is NOT merely a simple EaS scheme!
  - It fixes, intuitively, the problem that the simple EaS composition is not *generically secure* (since the signature part can reveal some information about plaintext as observed in [BN])

11

Flexible Public Key model

- Flexible Unsigncryption Oracle (FUO) model
  - Public key input for the unsigncryption oracle is *flexibly* given

Normal Unsigncryption Oracle: $USC_{y_A, x_B}^{G(.),H(.)}(.)$

Flexible Unsigncryption Oracle: $USC_{x_B}^{G(.),H(.)}(.)$

No specific sender's public key is given

12

FUO-IND-CCA2

- Confidentiality notion for signcryption with respect to adaptive chosen ciphertext attack (CCA2) under semantic security
- A CCA attacker has access to
  - the Flexible Unsigncryption Oracle, and
  - (fixed) Signcryption Oracle
    - (to be extended to flexible signcryption oracle (FSO) model in our forthcoming paper)

13

Another tool

- GAP Diffie-Hellman problem
  - Proposed by Okamoto & Pointcheval at PKC '01
  - Attacker searches the Diffie-Hellman key $g^{xy} \bmod p$ of $g^x \bmod p$ and $g^y \bmod p$ with the help of a decisional Diffie-Hellman Oracle,

$$DDH(g, g^x, g^y, W) = \begin{cases} 1 & \text{if } W = g^{xy} \bmod p \\ 0 & \text{otherwise} \end{cases}$$

14

Another tool (cont.)

- The GAP-DH problem is hard as long as there is no reduction from the DDH problem to the CDH (Computational DH) problem (-> The GAP-DH assumption)

- With the help of the DDH oracle, the flexible unsigncryption/signcryption oracles can be successfully simulated

15

Another tool (cont.)

- Actually, the GAP DH assumption is a *necessary condition* for some CCA-secure schemes to be proven (in our forthcoming paper)

16

“bind” information

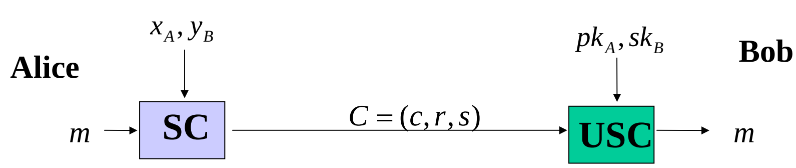
- “*bind*” info contains the sender Alice’s public key y_A and the receiver Bob’s public key y_B
  - It was pointed out by Zheng that this bind info should be included in the input to hash function H(.) to thwart “double spending attack”
  - This observation was crucial, as the “bind” information turned out to be necessary in proving the confidentiality of signcryption.

17

Signcryption scheme that we used in our formalization

Alice’s private/public key: $(x_A, y_A(= g^{x_A} \bmod p))$

Bob’s private/public key: $(x_B, y_B(= g^{x_B} \bmod p))$ $\quad bind = y_A \| y_B$



Signcryption

$c = ESYM_\tau(m)$,

$r = H(m \| bind \| \kappa)$,

$s = x/(r + x_A) \bmod q$

where $\tau = G(y_B{}^x \bmod p)$

$\kappa = y_B{}^x \bmod p$

UnSigncryption

$m = DSYM_\tau(c)$

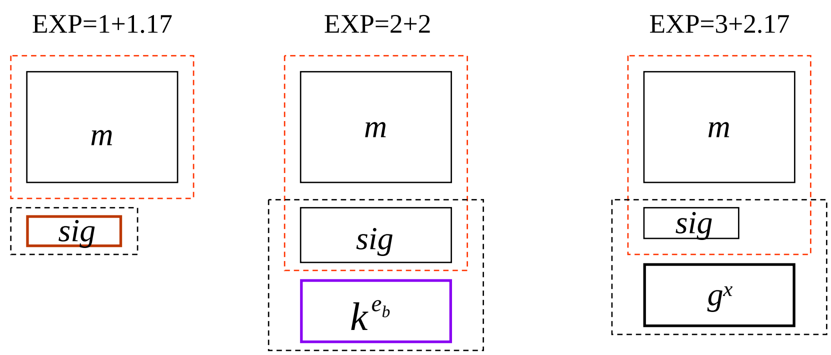
if $H(m \| bind \| \kappa) = r$

where $\tau = G((y_A g^r)^{sx_B} \bmod p)$

$\kappa = (y_A g^r)^{sx_B} \bmod p$

18

Signcryption v.s. Signature-then-Encryption

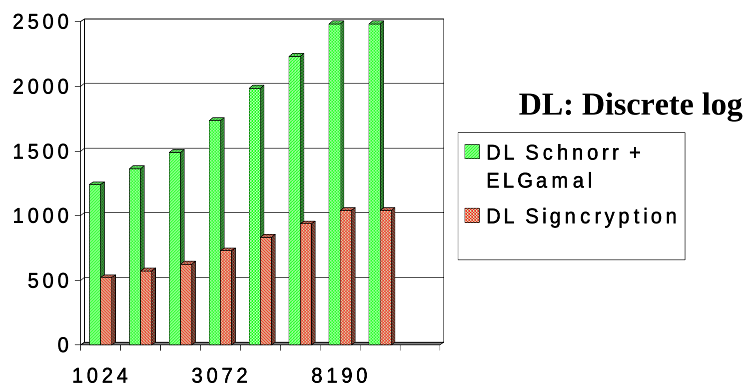


(a) Signcryption based on DL (b) Signature-then-Encryption based on RSA (c) Signature-then-Encryption based on DL

19

Time --- DL Signcryption v.s. DL Signature-then-Encryption

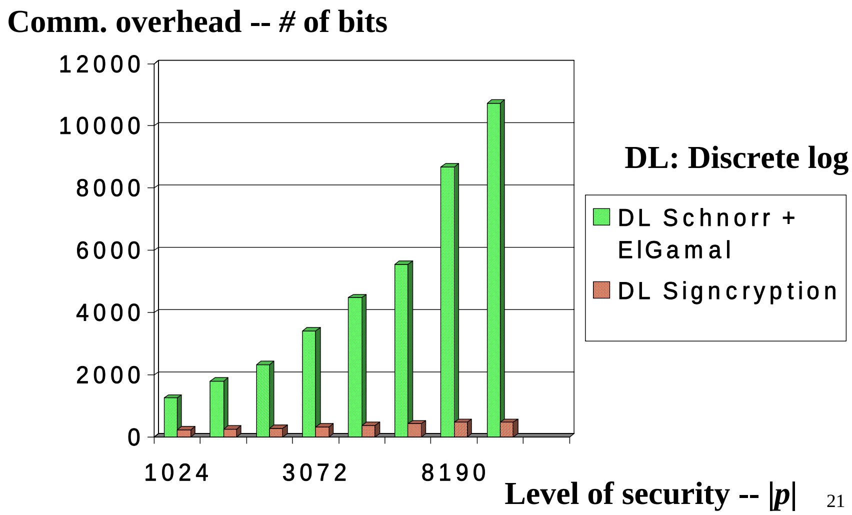
Time -- # of multiplications



Level of security -- |*p*|

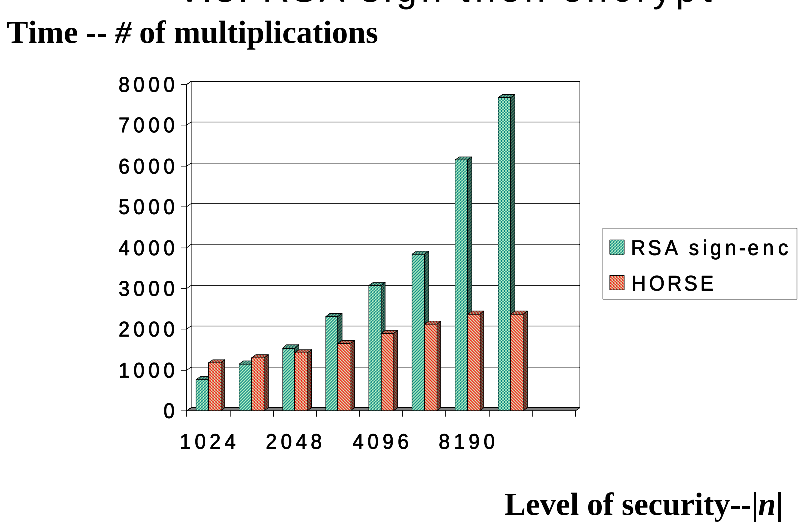
20

Bandwidth --- DL Signcryption v.s. DL Signature-then-Encryption



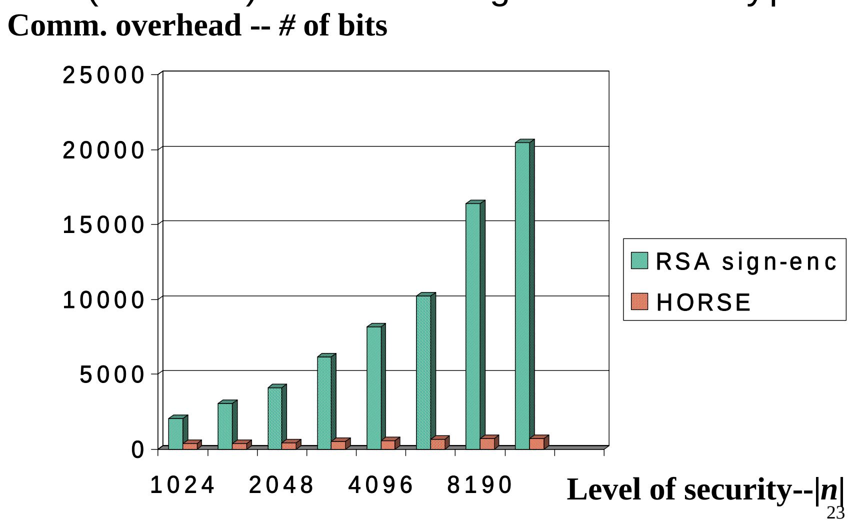
21

Time -- RSA signcryption (HORSE) v.s. RSA sign-then-encrypt



22

Bandwidth -- RSA signcryption (HORSE) v.s. RSA sign-then-encrypt



23

Confidentiality --- Sketch of proof

- An attacker (or an attack algorithm) for the GAP DH problem A_{gdh} runs adaptive chosen ciphertext attacker A_c to find the DH key $g^{xy} \bmod p$, given $g^x \bmod p$ and $g^y \bmod p$
- It is assumed that the A_c has access to the flexible unsigncryption oracle as well as the signcryption oracle
- The random oracles G and H, the signcryption/flexible unsigncryption oracle are successfully simulated with the help of the DDH oracle

24

Confidentiality --- Sketch of proof (cont.)

- When the events **Bad** and **GDHBrk** do not happen, we can construct a chosen plaintext attacker A_p which uses A_c as subroutine
  - **Bad**: The event which causes the distribution of A_c's view to differ in experiment in the simulation from the distribution of A_c's view in the real attack
  - **GDHBrk**: The event that A_c asks the DH key $g^{xy} \bmod p$ to the random oracle G or A_c asks a query *h* to the random oracle H where the k-rightmost bits of *h* is the DH key

Confidentiality --- Sketch of proof (cont.)

- As a result, we obtain the following upper bound:

$$\mathbf{Adv}_{\mathsf{SC}}^{\mathrm{fuo-ind-cca2}}(k, t, q_g, q_h, q_{sc}, q_{usc}) \leq 4\mathbf{Adv}_{\mathsf{GDH}}^{\mathrm{invert}}(k, t_1, q_{ddh}) + \mathbf{Adv}_{\mathsf{SC}^{\mathrm{SYM}}}^{\mathrm{ind-cpa}}(l, t_2, 0) + \frac{q_{sc}(q_g + q_h + 1) + q_{usc}}{2^{l_q(k)-1}}$$

All the variables are defined in our PKC02 paper

Confidentiality --- Sketch of proof (cont.)

- Maim Theorem 1:
  Signcryption is secure
  - against adaptive chosen ciphertext attacks
  - in the random oracle model
  - assuming the GAP Diffie-Hellman Problem is hard

27

Security notion for unforgeability of signcryption

- Follows the security notion for unforgeability of signcryption formulated by Steinfeld and Zheng (ISW '00)
- Allows the forger to have access to Bob's private key as well as the corresponding public key
  - Since signcryption offers non-repudiation for the sender Alice, it is essential that even the receiver Bob cannot impersonate Alice and forge valid signcrypted text from Alice to himself

28

Unforgeability --- Sketch of proof

- Convert a forger F which mounts chosen message attack on the signcryption scheme into an passive attacker A_i for the identification scheme derived from the signcryption scheme
- An attacker A_{dlp} for discrete logarithm problem uses A_i to solve the discrete logarithm associated with Alice's public key. (i.e., we use the ID-reduction technique by Ohta & Okamoto (Crypto '98))

29

Unforgeability --- Sketch of proof (cont.)

- As a result, we obtain the following upper bound:

$$\mathbf{Adv}_{\mathsf{SC}}^{\mathrm{cma}}(k, t, q_g, q_h, q_{sc}) \leq 2q_h \left(\mathbf{Adv}_{\mathsf{DLP}}^{\mathrm{search}}(k, t^*)\right)^{\frac{1}{2}} + \frac{1}{2^{l_q(k)}}$$

All the variables are defined in our PKC02 paper

30

Unforgeability --- Sketch of proof (cont.)

- Maim Theorem 2:
  Signcryption is existentially unforgeable
  - against adaptive chosen message attacks
  - in the random oracle model
  - assuming the Discrete Logarithm Problem is hard

31

Future work

- Providing the confidentiality proof using *FSO + FUO model*
- Providing the security proofs for various signcryption schemes proposed so far, including
  - Steinfeld-Zheng scheme (ISW ’00) based on integer factorization problem
  - Zheng scheme (PKC ’01) based on higher residuosity problem
  - Others …

32

Thank you very much!

감사합니다.