IEEE P1363 Meeting, UCSB
8/22/2002

Updates on Signcryption

Yuliang Zheng
UNC Charlotte

www.sis.uncc.edu/~yzheng
yzheng@uncc.edu

Signcryption

- Provides the functions of
  - digital signature
    - unforgeability & non-repudiation
  - public key encryption
    - confidentiality
- Has a significantly smaller comp. & comm. cost

Cost (signcryption) << Cost (signature) + Cost (encryption)

Signcryption -- public & secret parameters

- Public to all
  - p : a large prime
  - q : a large prime factor of $p-1$
  - g : $0<g<p$ & with order q mod p
  - G: 1-way hash
  - H: 1-way hash
  - (E,D) : private-key encryption & decryption algorithms

Alice's keys :

x_a : secret key

y_a : public key

$(y_a = g^{x_a} \bmod p)$

Bob's keys :

x_b : secret key

y_b : public key

$(y_b = g^{x_b} \bmod p)$

Signcryption -- 1st example

m $\longrightarrow$ **(*c*,*r*,*s*)** **(*c*,*r*,*s*)** $\longrightarrow$ ***m***

Signcryption by Alice :

1. Pick at random $x \in_R \{1,...,q-1\}$
2. $w = y_b^x \bmod p$
3. $k = G(w)$
4. $r = H(m, bind\_info, w)$
5. $s = x/(r + x_a) \bmod q$
6. $c = E_k(m)$
7. return (c, r, s)

Unsigncryption by Bob :

1. $w = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$
2. $k = G(w)$
3. $m = D_k(c)$
4. Return m if $r = H(m, bind\_info, w)$
5. Return "invalid" otherwise

Signcryption – 2nd example

m ⟶ ***(c,r,s)*** ***(c,r,s)*** ⟶ ***m***

Signcryption by Alice :

1. Pick at random $x \in_R \{1,...,q-1\}$
2. $w = y_b^x \bmod p$
3. $k = G(w)$
4. $r = H(m, bind\_info, w)$
5. $s = x/(1 + x_a \cdot r) \bmod q$
6. $c = E_k(m)$
7. return (c, r, s)

Unsigncryption by Bob :

1. $w = (g \cdot y_a^r)^{s \cdot x_b} \bmod p$
2. $k = G(w)$
3. $m = D_k(c)$
4. Return m if
   $r = H(m, bind\_info, w)$
5. Return "invalid" otherwise

Signcryption – 3rd example

m ⟶ ***(c,r,s)*** ***(c,r,s)*** ⟶ ***m***

Signcryption by Alice :

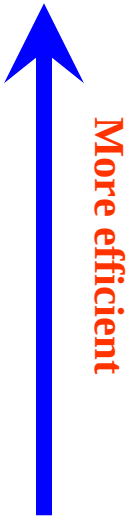
1. Pick at random $x \in_R \{1,...,q-1\}$
2. $w = y_b^x \bmod p$
3. $k = G(w)$
4. $r = H(m, bind\_info, w)$
5. $s = (x - x_a \cdot r) \bmod q$
6. $c = E_k(m)$
7. return (c, r, s)

Unsigncryption by Bob :

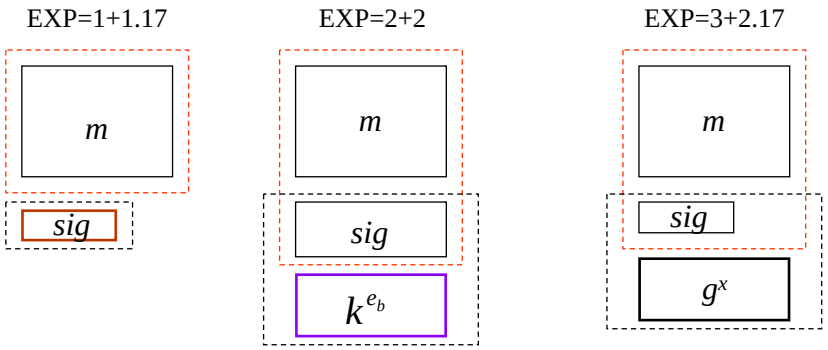
1. $w = (g^s \cdot y_a^r)^{x_b} \bmod p$
2. $k = G(w)$
3. $m = D_k(c)$
4. Return m if
   $r = H(m, bind\_info, w)$
5. Return "invalid" otherwise

Major instantiations of signcryption

- based on DL on an Elliptic Curve
  - Zheng, CRYPTO'97
  - Zheng & Imai IPL 1998
- based on other sub-groups (e.g. XTR)
  - Lenstra & Verheul, CRYPTO2000
  - Gong & Harn, IEEE-IT 2000
  - Zheng, CRYPTO'97
- based on DL on finite field
  - Zheng, CRYPTO'97
- based on factoring / residuosity
  - Steinfeld & Zheng, ISW2000
  - Zheng, PKC2001



Signcryption v.s. Signature-then-Encryption



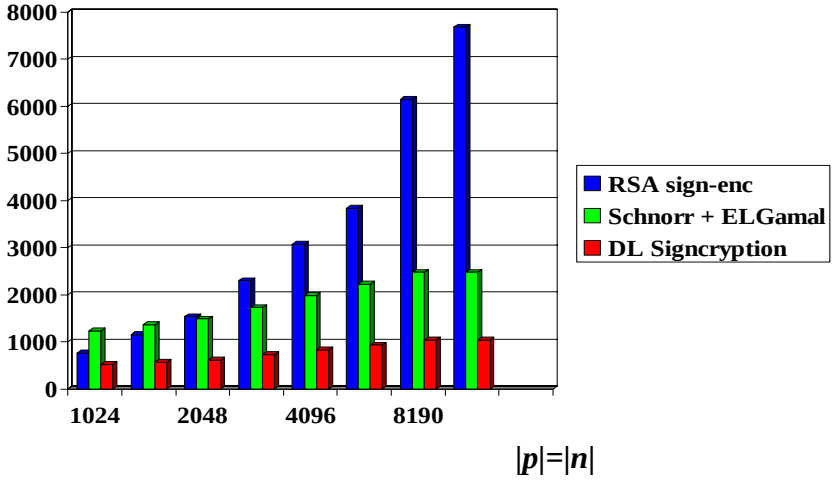
(a) Signcryption based on DL

(b) Signature-then-Encryption based on RSA

(c) Signature-then-Encryption based on DL

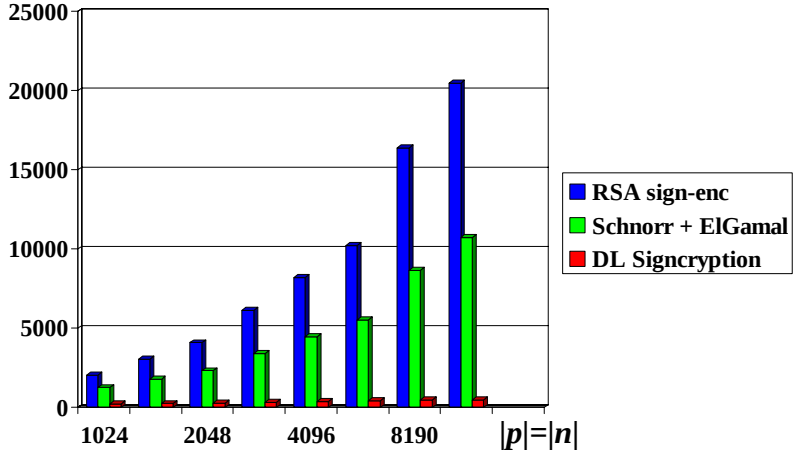
DL Signcryption v.s. sign-then-encrypt

# of multiplications



DL Signcryption v.s. sign-then-encrypt

comm. overhead (# of bits)



Security Proofs

- Analysis given in the Crypto'97 paper was informal
- In 2001,
  - Rigorous proofs (reductions) established
  - Results presented at PKC02 in Paris, Feb. 2002
  - Proof techniques applicable to signcryption schemes based on DL and EC

Standard assumptions

- Proofs for the confidentiality and unforgeability of signcryption
  - Confidentiality --- Providing a reduction
    - from breaking the security of signcryption with respect to adaptive chosen ciphertext attacks in the flexible public key model
    - to breaking the GAP Diffie-Hellman assumption, in the random oracle model
  - Unforgeability --- Providing a reduction
    - from breaking the unforgeability of signcryption against adaptive chosen message attacks
    - to the Discrete Logarithm problem, in the random oracle model

Updated documents

- Full version of the proof paper and updated descriptions of concrete signcryption schemes will be submitted to the IEEE P1363 website

Other developments

- Security proofs for combined signature and encryption including signcryption
- Parallel signcryption
- ID-based signcryption
- Threshold signcryption

Suggestions

- IEEE P1363 consider to standardize signcryption and other hybrid/combined schemes
- IEEE P1363-3 ?