



Some New Improved Signcryption Schemes

Jin-Woo Chung, Hong-Yeop Song

**Coding & Information Theory Laboratory
Dept. of Electrical and Electronic Engineering, Yonsei University**



Contents



- ◆ Signcryption Algorithm
- ◆ Defects of Signcryption
- ◆ Generalization of Signcryption
- ◆ Analysis of Generalized Signcryption
- ◆ Good Signcryption Schemes
- ◆ Conclusion



Signcryption Algorithm



Signcryption

$(C||s||r)$

Unsigncryption

$1 \leq x \leq q-1$

Select x arbitrarily
 $k = \text{hash}(y_b^x \pmod p)$

Split k into k_1 and k_2

$r = KH_{k_2}(m)$

signature { $s \equiv x / (r + x_a) \pmod q \rightarrow \text{SCS1}$
 $s \equiv x / (1 + x_a \cdot r) \pmod q \rightarrow \text{SCS2}$

encryption $\leftarrow C = E_{k_1}(m)$

SCS1 $\leftarrow k = \text{hash}((y_a \cdot g^r)^{s \cdot x_b} \pmod p)$

SCS2 $\leftarrow k = \text{hash}((y_a^r \cdot g)^{s \cdot x_b} \pmod p)$

Split k into k_1 and k_2

$D_k(C) = m \rightarrow \text{decryption}$

$KH_{k_2}(m)$

Accept m as valid if

$KH_{k_2}(m) = r$

signature verification



Defects of Signcrypton



Signcrypton

Select x arbitrarily

$$k = \text{hash}(y_b^x \pmod{p})$$

Split k into k_1 and k_2

$$r = KH_{k_2}(m)$$

$$s \equiv x / (r + x_a) \pmod{q} \quad \rightarrow \text{SCS1 : Defect 1, Defect 3}$$

$$s \equiv x / (1 + x_a \cdot r) \pmod{q} \quad \rightarrow \text{SCS2 : Defect 1, Defect 2, Defect 3}$$

$$C = E_{k_1}(m)$$

- ◆ Defect 1 : Division by zero.
- ◆ Defect 2 : Vulnerable to Attack.
- ◆ Defect 3 : Division algorithm required.



Generalization of Signcrypton



Signcrypton

Select x arbitrarily

$k = \text{hash}(y_b^x \pmod{p})$ → **Must we use one-way hash function?**

Split k into k_1 and k_2 → **Is splitting k necessary?**

$r = KH_{k_2}(m)$ → **Must we use keyed hash function?**

$s \equiv x / (r + x_a) \pmod{q}$
 $s \equiv x / (1 + x_a \cdot r) \pmod{q}$ } **Is it possible to generalize the calculation of s ?**

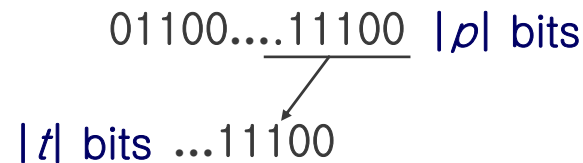
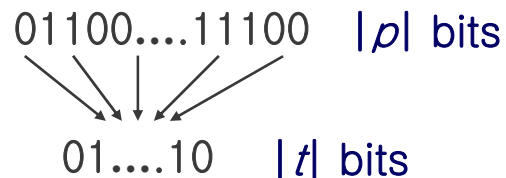
$C = E_{k_1}(m)$



A hash function for k

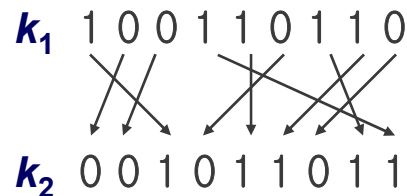


- ◆ In the calculation of $k = \text{hash}(y_b^x \pmod p)$, must we use a one-way hash function?
- ◆ k is a **secret** parameter. **Therefore, we do not have to use a hash function.**
- ◆ Use of a hash function can be generalized to **arbitrary function $h : \mathbb{Z}_p \rightarrow \mathbb{Z}_t$** .
 - **Example**) Define function h as selecting $|t|$ bits from $y_b^x \pmod p$



Splitting k

- ◆ Is splitting k the only way to obtain k_1 and k_2 ?
- ◆ One of the simple ways is choosing $k=k_1$ and obtain k_2 from k_1 .
 - Example 1) Let $k = 100110110$. Then $k_1=k$.



- Example 2) Select $k_1=k_2=k$.



A keyed hash function for r



- ◆ In the calculation of $r = KH_{k_2}(m)$, must we use a keyed hash function ?
- ◆ A key-less hash function can also be used instead of a keyed hash function.
- ◆ If a keyed hash function is used, then additional computational cost is needed.



Derivation of Signature Equation



◆ Calculation of s

EIGamal-type

$$A \equiv x_a B + xC \pmod{q}$$

$$g^A \equiv y_a^B \cdot r^C \pmod{p}$$

$$r \equiv d(g^{A \cdot C^{-1}} \cdot y_a^{-B \cdot C^{-1}} \pmod{p}), m)$$

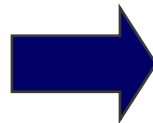
where $A, B, C \in \{1, \pm r, \pm m, \pm s, \pm f(m, r), \pm f(m, s), \pm f(r, s)\}$

Signature Equation

Verification Equation

$$d: \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p$$

Signcryption



$$A \equiv x_a B + xC \pmod{q}$$

◆ Recovery of k

$$k = h(g^{A \cdot C^{-1} \cdot x_b} \cdot y_a^{-B \cdot C^{-1} \cdot x_b} \pmod{p})$$



Signature Equation $A \equiv x_a B + xC \pmod{\dots}$



$$A, B, C \in \{1, \pm r, \pm m, \pm s, \pm f(m, r), \pm f(m, s), \pm f(r, s)\}$$

- ◆ Conditions for simplicity
 1. The message value **m is eliminated.**
 $\Rightarrow A, B, C \in \{1, \pm r, \pm s, \pm f(r, s)\}$
 2. The operation f is confined to **modulo addition or multiplication.**
 3. One of the parameters A, B, C **equals to 1.**



$$\text{◆ Possible choices of } A, B, C \\ (1, r, s), (1, r, r+s), (1, r, r \cdot s), (1, s, r+s), (1, s, r \cdot s)$$

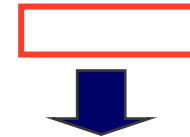


Analysis of Generalized Signcrypton



A	B	C	Signature Equation	Calculation of s	D1	D2	D3
1	r	s	$1 \equiv x_a \cdot r + x \cdot s$	$s \equiv (1 - x_a \cdot r) / x$	X	1,2	2
1	s	r	$1 \equiv x_a \cdot s + x \cdot r$	$s \equiv (1 - x \cdot r) / x_a$	X	2,1	2
r	1	s	$r \equiv x_a + x \cdot s$	$s \equiv (r - x_a) / x$	X	1	2
r	s	1	$r \equiv x_a \cdot s + x$	$s \equiv (r - x) / x_a$	X	1	1
s	1	r	$s \equiv x_a + x \cdot r$	$s \equiv x_a + x \cdot r$	X	1	1
s	r	1	$s \equiv x_a \cdot r + x$	$s \equiv x_a \cdot r + x$	X	1	X
1	r	$r+s$	$1 \equiv x_a \cdot r + x \cdot (r+s)$	$s \equiv (1 - x_a \cdot r - x \cdot r) / x$	X	1,3	2
1	$r+s$	r	$1 \equiv x_a \cdot (r+s) + x \cdot r$	$s \equiv (1 - x \cdot r - x_a \cdot r) / x_a$	X	3,1	2
r	1	$r+s$	$r \equiv x_a + x \cdot (r+s)$	$s \equiv (r - x_a - x \cdot r) / x$	X	3	2
r	$r+s$	1	$r \equiv x_a \cdot (r+s) + x$	$s \equiv (r - x - x_a \cdot r) / x_a$	X	3	1
$r+s$	1	r	$r+s \equiv x_a + x \cdot r$	$s \equiv x_a + x \cdot r - r$	X	1	1
$r+s$	r	1	$r+s \equiv x_a \cdot r + x$	$s \equiv x_a \cdot r + x - r$	X	1	X
1	r	$r \cdot s$	$1 \equiv x_a \cdot r + x \cdot (r \cdot s)$	$s \equiv (1 - x_a \cdot r) / (x \cdot r)$	1	2	2
1	$r \cdot s$	r	$1 \equiv x_a \cdot (r \cdot s) + x \cdot r$	$s \equiv (1 - x \cdot r) / (x_a \cdot r)$	1	2	2
r	1	$r \cdot s$	$r \equiv x_a + x \cdot (r \cdot s)$	$s \equiv (r - x_a) / (x \cdot r)$	1	1	2
r	$r \cdot s$	1	$r \equiv x_a \cdot (r \cdot s) + x$	$s \equiv (r - x) / (x_a \cdot r)$	1	1	1
$r \cdot s$	1	r	$r \cdot s \equiv x_a + x \cdot r$	$s \equiv (x_a + x \cdot r) / r$	1	X	2
$r \cdot s$	r	1	$r \cdot s \equiv x_a \cdot r + x$	$s \equiv (x_a \cdot r + x) / r$	1	X	1
1	s	$r+s$	$1 \equiv x_a \cdot s + x \cdot (r+s)$	$s \equiv (1 - x \cdot r) / (x_a + x)$	E	1,3	2
1	$r+s$	s	$1 \equiv x_a \cdot (r+s) + x \cdot s$	$s \equiv (1 - x_a \cdot r) / (x_a + x)$	E	3,1	2
s	1	$r+s$	$s \equiv x_a + x \cdot (r+s)$	$s \equiv (x_a + x \cdot r) / (1 - x)$	E	3	2
s	$r+s$	1	$s \equiv x_a \cdot (r+s) + x$	$s \equiv (x_a \cdot r + x) / (1 - x_a)$	E	3	1
$r+s$	1	s	$r+s \equiv x_a + x \cdot s$	$s \equiv (x_a - r) / (1 - x)$	E	1	2
$r+s$	s	1	$r+s \equiv x_a \cdot s + x$	$s \equiv (x - r) / (1 - x_a)$	E	1	1
1	s	$r \cdot s$	$1 \equiv x_a \cdot s + x \cdot (r \cdot s)$	$s \equiv 1 / (x_a + x \cdot r)$	2	1	2
1	$r \cdot s$	s	$1 \equiv x_a \cdot (r \cdot s) + x \cdot s$	$s \equiv 1 / (x_a \cdot r + x)$	2	1	2
s	1	$r \cdot s$	$s \equiv x_a + x \cdot (r \cdot s)$	$s \equiv x_a / (1 - x \cdot r)$	2	1	2
s	$r \cdot s$	1	$s \equiv x_a \cdot (r \cdot s) + x$	$s \equiv x / (1 - x_a \cdot r)$	2	1	1
$r \cdot s$	1	s	$r \cdot s \equiv x_a + x \cdot s$	$s \equiv x_a / (r - x)$	1	X	2
$r \cdot s$	s	1	$r \cdot s \equiv x_a \cdot s + x$	$s \equiv x / (r - x_a)$	1	X	1

$$A \equiv x_a B + xC \pmod{q}$$



Good Signcrypton Scheme
 (Having only one defect,
 detection speed is fast and
 number of division is less
 than or equal to 1.)

D1, D2, D3 : Defect 1, 2, 3

X : No defect

in D1, D2 : Detection speed.

in D3 : Number of division.

E : Easily Avoided



Good Signcryption Schemes

A	B	C	GSCSs	Defect 1 or 2 (if $r \neq 0$)	no. of div.	Comment
s	1	r	YES	None if $r \neq 0$	1	*
s	r	1	YES	None if $r \neq 0$	0	ISCS1 *
$r + s$	1	r	YES	None if $r \neq 0$	1	*
$r + s$	r	1	YES	None if $r \neq 0$	0	ISCS2 *
$r \cdot s$	r	1	YES	None if $r \neq 0$	1	*
$r \cdot s$	1	r	NO	None if $r \neq 0$	2	
r	s	1	YES	Defect 2 even if $r \neq 0$	1	
$r + s$	s	1	YES	Defect 2 even if $r \neq 0$	1	
s	$r \cdot s$	1	NO	Defect 1 even if $r \neq 0$	1	SCS2
$r \cdot s$	s	1	YES	Defect 1 even if $r \neq 0$	1	SCS1

- ◆ 5 GSCSs can overcome both Defect 1 and 2 when modification of a hash function is used.
- ◆ 2 GSCSs can overcome all three defects, which are called **Improved Signcryption Schemes (ISCSs)**.



Conclusion



- ◆ The 5 GSCSs marked with * are good enough.
- ◆ For 2 ISCSs, all 3 defects are eliminated by using a hash function that does not have zero as its output.