Okamoto - Injected Ephemerals

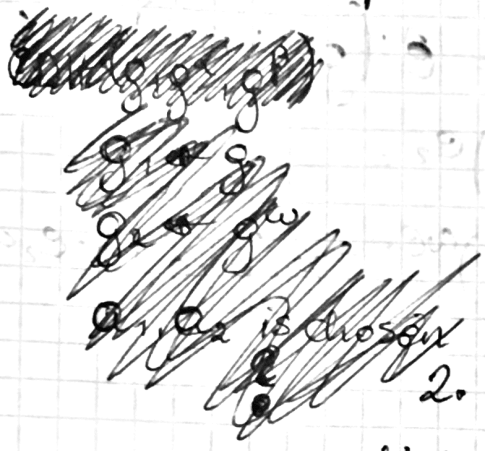
(ParamGen, KeyGen, P, V), Π.

1. Correctness

$$\Pi\left(P^{X}(a,A), V(A)\right) \to 1$$

2. Security

Exp: 1. Init



params ← ParamGen

sk, pk ← KeyGen(params)

2. Query Stage

active $\Pi\left(P^{X}(sk,pk), V(pk)\right) \rightsquigarrow V^1$

$\vdots$

V^L

$\Pi\left(P^{X}(sk,pk), V(pk)\right) \rightsquigarrow T^1$

$\vdots$

T^L

3. Impersonation

$\Pi\left(ct(V,pk), V(pk)\right) \rightsquigarrow res$

$Adv(ct, Exp) = P[\quad]$

Protocol secure if ... $\leq negl()$

$P(sk = a_1, a_2, pk = A)$ $\qquad$ $V(A)$

$x_1, x_2 \leftarrow rand$

$X = g_1^{x_1} g_2^{x_2}$ $\xrightarrow{X}$

$\qquad\qquad g_2 = g_1^{\omega}$

$\qquad\qquad c \leftarrow \mathbb{Z}_q^*$

$\xleftarrow{c}$

$\hat{g} = \mathcal{H}(X \| C)$

$s_1 = \hat{g}^{x_1 + a_1 c}$

$s_2 = \hat{g}^{x_2 + a_2 c}$ $\xrightarrow{s_1, s_2}$ $\hat{e}(s_1, g_1) \cdot \hat{e}(s_2, g_2) =$

$= \hat{e}(\hat{g}, X A^c)$

1. Correctness $\quad e(a^c, b) = e(a,b)^c$

$$\hat e(\hat g^{x_1+a_1c}, g_1)\cdot \hat e(\hat g^{x_2+a_2c}, g_2) =$$

$$= \hat e(\hat g, g_1^{x_1+a_1c}) \cdot \hat e(\hat g, g_2^{x_2+a_2c}) =$$

$$= \hat e(\hat g, g_1^{x_1+a_1c}) \cdot \hat e(\hat g \ldots = \hat e(\hat g, XA^c), \text{ bo}$$

$$\hat e(\hat g, g_1)^{e_1} \hat e(\hat g, g_2)^{e_2} =$$

$$= \hat e(\hat g, g_1)^{e_1} \hat e(\hat g, g_1)^{\omega e_2} = \hat e(\hat g, g_1^{e_1+e_2\omega})$$

2. Security

1. Init

$g_1 \leftarrow g$ $\quad$ CDH(g, g^α, g^β)

$g_2 \leftarrow g^\omega$ $\quad$ β is given

We choose

$a_2, \omega \leftarrow \mathbb{Z}_q$

$A \leftarrow g^\alpha = g_1^{a_1} g_2^{a_2}$

chosen $\quad$ unknown

2. Simulation

passive

$\xrightarrow{X}$

$\xleftarrow{c}$

$\xrightarrow{s_1, s_2}$

wyrocznia losowe $\quad$ $e(s_1, g_1) e(s_2, g_2) =$

daje $\quad g = g^r$ $\quad$ $e(g^r, XA^c)$

s_1, s_2 losowo, c losowo

exp $\quad g_1^{s_1} \cdot g_2^{s_2} = (XA^c)^r \rightarrow$ 2malerz

X

active

wyrocznia daje g^r

$g_1^{x_1}, g_2^{x_2}$ $\xrightarrow{x}$ $\xleftarrow{c}$

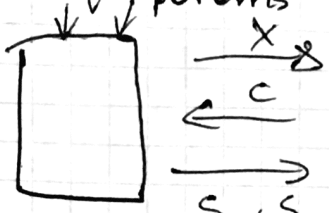
$\hat{g} \leftarrow g^r$

$S_1 = (g^r)^{x_1} \left(A / g_1^{a_2 w}\right)^c = \hat{g}^{x_1 + a_2 c}$

Jak? g_1^a

$S_2 = g^{r(x_2 + a_2 c)}$

3o Impersonation



DL-ROM

$S_1 = (g^r)^{x_1 + a_1 c} =$

$= (g^r)^{x_1} \cdot (g^r)^{a_1 c} =$

$= (g_1^r)^{x_1} (g_1^{a_1})^{cr} =$

$= (g_1^r)^{x_1} \left(\frac{A}{g_1^{a_2 w}}\right)^{cr}$

PROM $g^{\beta r}$

$S_1 = \hat{g}^{x_1 + a_1 c} = (g^\beta)^r (x_1 + a_1 c)$

$S_2 = \hat{g}^{x_2 + a_2 c} = (g^\beta)^r (x_2 + a_2 c)$

$S_1' = g^{\beta r' (x_1' + a_1' c')}$

$S_2' = g^{\beta r' (x_2' + a_2' c')}$

$\bar{S}_1 = S_1^{\frac{1}{r}}$ $\quad \bar{S}_1' = \bar{S}_1'^{\frac{1}{r'}}$

$\bar{S}_2 = S_2^{\frac{1}{r}}$ $\quad \bar{S}_2' = \bar{S}_2'^{\frac{1}{r'}}$

$g^{x_1} \cdot g^{x_2 w} = X$

$g^{x_1'} \cdot g^{x_2' w} = X$

$\left(\frac{\bar{S}_1 \cdot \bar{S}_2^{\,w}}{\bar{S}_1' \cdot \bar{S}_2'^{\,w}}\right)^{\frac{1}{c - c'}} = g^{\alpha - \beta}$

$e(g, g^\alpha)^\alpha \cdot e(g, g^\beta)^\beta = e(g, g^{\alpha\beta})$

$e(g, g)^{\alpha + \beta} = e(g, g^{\alpha + \beta})$