$\mathcal{P}$
$\mathcal{V}$

$\mathcal{V}$
$\mathcal{V}$

$\mathcal{V}$

$\mathcal{V}$

$\mathcal{P}$

$\mathcal{V}$

$\mathcal{P}$ $\mathcal{V}$

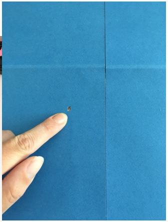
$\mathcal{V}$

$\mathcal{V}$ $\mathcal{P}$

$\mathcal{P}$

$\mathcal{V}$

$\mathcal{P}$ 50%



$\mathcal{L} \in \mathit{NP}$

$\mathcal{M}$

$\in \mathcal{L} \Leftrightarrow \exists \in \{0,1\}^{(||)} : (,) = 1$

$\mathcal{P}\,\mathcal{V}$

$\langle \mathcal{P}(,), \mathcal{V}() \rangle \mathcal{P}\,\mathcal{V}\,\mathcal{P}$

$\nu \langle \mathcal{P}(,), \mathcal{V}() \rangle \mathcal{V}$

$\mathcal{L}$

$= \langle, : \langle\rangle = \mathbb{Z}^*, \in \mathbb{Z}^*\rangle$

$: \; =$

$\mathcal{L}\langle\mathcal{P}(,),\mathcal{V}()\rangle$

$\mathcal{P}\,\mathcal{V}$
$\in \mathcal{L}(,) = 1$

$$[\nu\langle\mathcal{P}(,),\mathcal{V}()\rangle() = 1] = 1$$

$\mathcal{P}\mathcal{P}^*\mathcal{V} \notin \mathcal{L}\forall(\mathcal{P}^*, ^*)$

$$[_{\mathcal{V}}\langle\mathcal{P}^*(, ^*), \mathcal{V}()\rangle() = 1] = (\lambda)$$

$\mathcal{P}^*$

$\mathcal{P}^*\mathcal{E}\mathcal{V}$

$\mathcal{V}\mathcal{P}$

$\mathcal{V}\mathcal{P}$

$\mathcal{S}$

$\mathcal{P}$

$\mathcal{V}^*\mathcal{S} \in \mathcal{L}(,) = 1$

$$\mathcal{V}^* \langle \mathcal{P}(,), \mathcal{V}^*()\rangle()$$

$$\mathcal{V}^* \langle \mathcal{S}(), \mathcal{V}^*()\rangle()$$

$\mathcal{P}$

$\mathcal{V}$

$\langle \mathcal{S}\,\mathcal{V} \rangle \langle \mathcal{P}\,\mathcal{V} \rangle$

$\mathcal{V}\,\mathcal{S}$

$\mathcal{V}$

$\mathcal{P}\,\mathcal{S}$

$\mathcal{S}$

$\mathcal{V}\,\mathcal{P}\,\mathcal{S}$

$\mathcal{SP}^*$

$\mathcal{P}^*$ $\mathcal{S}$

$\mathcal{V}^*$

$\mathcal{V}$

$\mathcal{P}_1, \mathcal{P}_2$

$\mathcal{V}^*$

$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_1$

$\exists\mathcal{S}\ \forall\mathcal{V}^*$

$_{\mathcal{V}^*}\langle\mathcal{P}(,),\mathcal{V}^*()\rangle()_{\mathcal{V}^*}\langle\mathcal{S}^{\mathcal{V}^*}(),\mathcal{V}^*()\rangle()$

$\mathcal{S}$

$\mathcal{V}$

$\mathcal{V}$

$\mathcal{P}$,

.

$\Delta(,) = \frac{1}{2}\sum_{\in} |_{[} =] - [=]| = (\lambda)$

$\mathcal{V}$

$\mathcal{P}$

$\mathcal{S}\left\langle \mathcal{P}(,), \mathcal{V}()\right\rangle$

$\mathcal{V}$

$\mathcal{V}$

$\mathcal{S}$

$\mathcal{V}$

$\mathcal{VP}$

$\mathcal{E}\mathcal{P}\mathcal{V}$

$\Rightarrow \frac{1}{||}\mathcal{V}$

$\Rightarrow$

$$_0 = (_0, _0)_1 = (_1, _1)|_0| = |_1|$$

$$_0 \cong {}_1\pi : {}_0 \to {}_1(,) \in {}_0 \Leftrightarrow (\pi(), \pi()) \in {}_1$$

$0, 1$

π

$\mathcal{P}\, \pi_{11}$

$_1 \cong \mathcal{V}$

$\mathcal{V}$

$= 1\phi = \pi_1 : {}_1 \to$

$= 0\phi = \pi_1 . \pi : {}_0 \to {}_0 \cong$

$\mathcal{V}\, \phi() =$

$\mathcal{P}, \mathcal{V}$

$$= 1 : \phi() = \pi_1(_1) =$$

$$= 0 : \phi() = \pi_1 . \pi(_0) = \pi_1(_1) =$$

$\mathcal{P}\, \pi_0 \cong {}_1$

$$\mathcal{V}\, \tfrac{1}{2} \mathcal{P}\,^* \phi_0 \phi_1$$

$\mathcal{S}$

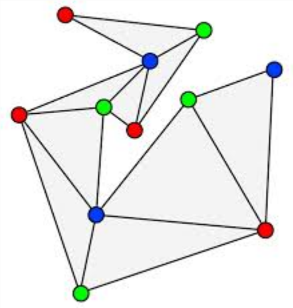
$'\pi'$

$= \pi'(,)$

$= '\pi'$

2^{-}

$\sum_{=1}^{\infty} 2^{-} =$



$$= (,)$$

$$\mathcal{P} : \to \{1, 2, 3\}$$

$$(,) \in \Rightarrow () \neq ()$$

$\mathcal{P}\,\pi\{1,2,3\}$

$\pi.$

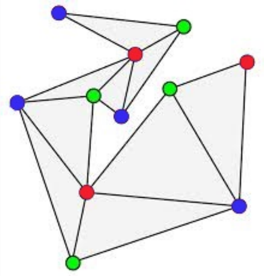
$((\pi.)(),)\forall \in$
$\mathcal{V}$

$\mathcal{V}\,(,) \in \mathcal{P}$

$\mathcal{P}\,\pi.(),\pi.(),$

$\mathcal{V}\,\pi.() \neq \pi.()$

$||^2$



$\pi.$

$\mathcal{V}$

$\mathcal{P}^*$

$\mathcal{V}\,\frac{1}{||}$
$\mathcal{P}^* 1 - \frac{1}{||}$
$||^2$

$$(1 + \ ) \leq$$

$\mathcal{P}^*$

$$(1 - \tfrac{1}{||})^{||^2} \leq {}^{-||}$$

$\mathcal{S}$

$\mathcal{S}$

$\mathcal{V}^{\frac{2}{3}}$

$\mathcal{V}^{\frac{1}{3}}$

$\mathcal{V}$

$\underline{3/2}$

$\mathcal{S}\,\mathcal{P}$

$\mathcal{P}\,\mathcal{S}$

$\mathcal{P}$

$\mathcal{V}$

$\mathcal{P}$

$\mathbb{Z}^* \in \mathbb{Z}^*$

$\mathcal{P} \in \mathbb{Z}^* = \pmod{}$

$$\{() : = \pmod{}, , \in \mathbb{Z}^*\}$$

$\mathcal{P} \rightarrow \mathcal{V}$

$\in \mathbb{Z}^*$

$=$ mod

$\mathcal{V}$

$\mathcal{V} \rightarrow \mathcal{P}$

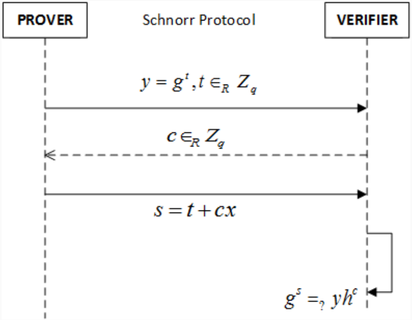
$\in \mathbb{Z}^*$

$\mathcal{P} \rightarrow \mathcal{V}$

$\mathcal{P} = +$ mod $\mathcal{V}$

$\mathcal{V}$

$=$ (mod)



$$= {}^{+} = \quad = \quad \pmod{\ }$$

$\mathcal{P}$ * [1]

$(,,)(,',')$

$$= ' = ' \Rightarrow - = '-' \Rightarrow$$
$$- = '-' \Rightarrow - = ' - ' \Rightarrow$$
$$= \frac{' -}{-}$$

$\mathcal{P}$

$\mathcal{S}\,\mathcal{V}$

$\mathcal{S} \;=\; , \;\in \mathbb{Z}^*$

$\mathcal{V} \;\in \mathbb{Z}^*$

$\mathcal{S}$

$\mathcal{V}$

$\mathcal{S} \;=\; ^-, \;\in \mathbb{Z}^*$

$\mathcal{V} \;\in \mathbb{Z}^*$

$\mathcal{S} \;=$

$\mathcal{V}$

$= \,^- = \;=$

$(\;\in \mathbb{Z};\, ^-, \;\in \mathbb{Z}, \,)(, \;\in \mathbb{Z};\, ,\, , \;+ \,)$

$\mathcal{S}$

$\mathcal{S}$

$\mathcal{V}\mathcal{P}$

$\{0, 1\}$

$\mathcal{V}$

$\mathcal{S}$

$_1, _2 \mathbb{Z}^* {}_1, {}_2 \in \mathbb{Z}^*$

$\mathcal{P} \in \mathbb{Z}_1 = {}_1 \bmod {}_2 = {}_2 \bmod$

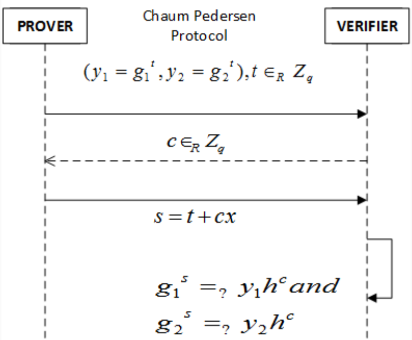
$$\{() : {}_1 = {}_1 \pmod{} \wedge {}_2 = {}_2 \pmod{}, {}_1, {}_1, {}_2, {}_2 \in \mathbb{Z}^*\}$$

$\mathcal{P} \in \mathbb{Z}$

$_1 = {}_1 \bmod$

$_2 = {}_2 \bmod$

$_1, {}_2 \mathcal{V}$



$\mathcal{V} \in \mathbb{Z}$

$\mathcal{P} = + \bmod \mathcal{V}$

$$\mathcal{V}_1 = {}_{11} \pmod{}_2 = {}_{22} \pmod{}$$

$_1 = {}_12 = {}_2$

$$_1 = {}^+_1 = {}_1{}_1$$
$$_2 = {}^+_2 = {}_2{}_2$$

$((_1, {}_2), ,)((_1, {}_2), ', ')$

$$_1 = {}_1{}_1{}_1' = {}_1{}_1' \Rightarrow {}_1{}_1^- = {}_1'{}_1^{-'}$$
$$_2 = {}_2{}_2{}_2' = {}_2{}_2' \Rightarrow {}_2{}_2^- = {}_2'{}_2^{-'}$$

$= \frac{-'}{'-}$

$\in \mathbb{Z}$

$$(\in \mathbb{Z}; (_1, _2), \in \mathbb{Z}, + \mod)$$

$\in \mathbb{Z}$

$$(, \in \mathbb{Z}; (_1 \bar{1}, _2 \bar{2}), ,)$$

$= {}_1 1 = {}_2 2$

$(, ,) =$
$CP(_1 = , _2 = , _1 = , _2 = \ = \ )$

$\mathbb{Z}^*(_1, _2)$

$$(_1, _2) = (, \ \cdot \ )$$

$$_1 = (\frac{2}{})$$

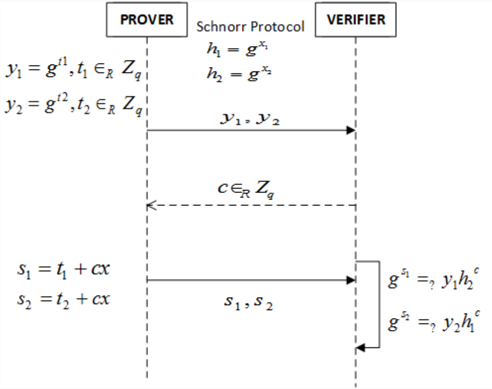
$\mathcal{P}$

Σ

AND

$\mathcal{P}$

Σ



$(,,)(,,)$
$(,,)$

EQ

$\mathcal{P}$

OR

$\mathcal{P}$

$= \{_1, ..., \}$

$\mathcal{P}$

$\mathcal{P}\,\mathcal{S}\,\mathcal{V}$

$\mathcal{S}$

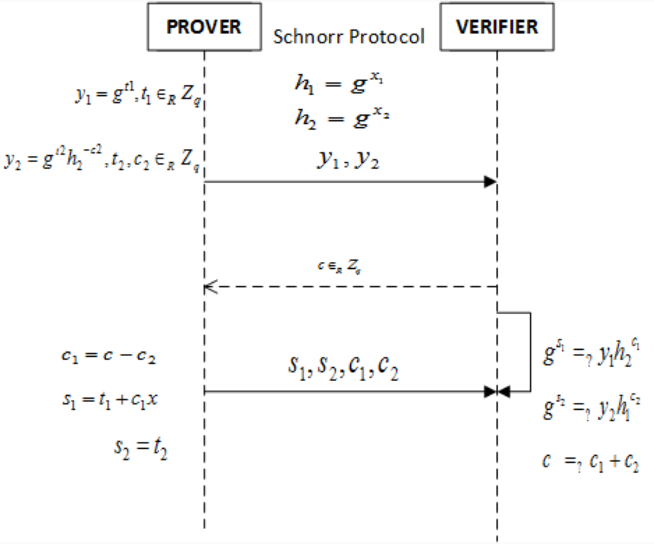
$\mathcal{V}$

$\mathcal{P}$

$\mathcal{P}$

$\mathcal{V}$

$$\{(_1, _2) : {}_1 = {}^1_1 \pmod{} \vee {}_2 = {}^2_2 \pmod{}\}\mathcal{P}\,_1$$



$\mathcal{V}$
$\mathcal{P}$

$\mathcal{P}, \mathcal{V}$

$\mathcal{H}$

$\mathbb{Z}^* \in \mathbb{Z}^*$

$\mathcal{P} \in \mathbb{Z}^* = \mod$

$\mathcal{P}$

$\in \mathbb{Z}$

$= \mod$

$= \mathcal{H}()\mathcal{H}\mathbb{Z}$

$= + \mod$

$(,,)$

$= \mathcal{H}(^-)$

$\mathcal{V}^*$

$() = \{ : (,) = 1\}$

$\mathcal{P}\mathcal{V} \in ()$

$\mathcal{V}^*$

$\mathcal{V}^* \in ()$

$\mathcal{V}^* \in ()\mathcal{P}$

$\to\to$

$\to$

$\to$

$\not\to$

$\forall \mathcal{V}^*$

$$\{\langle \mathcal{P}\,(), \mathcal{V}^*()\rangle()\}_{\in,\in()} \equiv \{\langle \mathcal{P}\,('), \mathcal{V}^*()\rangle()\}_{\in,'\in()}$$

$\mathbb{G}_{1,\,2} \in \mathbb{G} \in \mathbb{G}_{1,\,21,\,2} \in \mathbb{Z} = {}^{1\,2}_{12}$

$1,221$

$$\{(_1, _2) : \ = {}^{1\,2}_{12}, \mathbb{G}, , \ _1, _2, \ \in \mathbb{G}, \}$$

$\mathcal{P}\ _1, _2 \leftarrow \mathbb{Z}$

$\leftarrow {}^{1\,2}_{12}$

$\mathcal{V} \leftarrow \mathbb{Z}$

$\mathcal{P}\ _1 = \ _1 + \ _{12} = \ _2 + \ _2$

$_1, _2$

$\mathcal{V}\ {}^{1\,2}_{12} =$

$$= {}_1^{\,{}_1}{}_2^{\,{}_2} = {}_1^{\,{}'_1}{}_2^{\,{}'_2}$$

$${}_1^{\,{}_1-{}'_1}\,{}_2^{\,{}_2-{}'_2} = {}^{-1} = 1$$

$(,,{}_1,{}_2)\,{}_1,{}_2\,{}_1,{}_2\,{}'_1,{}'_2\,{}'_1,{}'_2$

$$\begin{aligned}
{}'_1 &= {}_1 + ({}_1 - {}'_1) \\
{}'_2 &= {}_2 + ({}_2 - {}'_2) \\
{}' &= {}_1^{\,{}'_1}{}_2^{\,{}'_2} = {}_1^{\,{}_1+({}_1-{}'_1)}\,{}_2^{\,{}_2+({}_2-{}'_2)} = \\
&= {}_1^{\,{}_1}{}_2^{\,{}_2}\,{}_1^{\,({}_1-{}'_1)}\,{}_2^{\,({}_2-{}'_2)} = \\
&=
\end{aligned}$$