De Cifris Trends
in
Cryptographic Protocols

University of Trento and *De Componendis Cifris*

October 2023

Michele Ciampi The University of Edinburgh

Sigma Protocols

Michele Ciampi

The University of Edinburgh

michele.ciampi@ed.ac.uk

Sigma protocols

Thm: x

$P_\Sigma(x,w)$ $\qquad$ $V_\Sigma(x)$

$$a' \quad \equiv \quad \xrightarrow{a}$$
$$c' \quad \equiv \quad \xleftarrow{c}$$
$$z' \quad \equiv \quad \xrightarrow{z}$$

- Completeness
- Honest Verifier Zero-Knowledge

$\mathcal{HVZK}_{Sim}(x) \Rightarrow$

- Special Soundness

$\boxed{\mathbf{x}, (\mathbf{a}\ c\ z)}$

$\boxed{\mathbf{x}, (\mathbf{a}\ c'\ z')}$

$c \neq c' \Rightarrow$ $\boxed{w: (\mathbf{x}, w) \in R}$

Sigma protocol for Discrete Logarithm

Let G be a group of order q, with generator g

$y \leftarrow Z_q$
$x = g^y$

$\xrightarrow{(G,g,x)}$

$\xleftarrow{y'}$

$\mathrm{Prob}[y' = y] = \mathrm{negl}(q)$

Schnorr protocol

Let G be a group of order q, with generator g

$x = g^{y}$

y

$a = g^r$

c

$z = r + cy$

Accept iff $g^z = ax^c$

$g^z = g^{r+cy}$ $\quad ax^c = g^r g^{yc} = g^{r+cy}$

Special-soundness

a

c $\quad c'$

z $\quad z'$

$$\begin{cases} z = r + cy \\ z' = r + c'y \end{cases} \xrightarrow{c \neq c'} y$$

Michele Ciampi The University of Edinburgh

Schnorr protocol

$x = g^y$

y

$a = g^r$

c

$z = r + cy$

Accept iff $g^z = ax^c$

HVZK

$\mathcal{HVZK}_{sim}$

$c \Leftarrow Z_q$

$z \Leftarrow Z_q$

$a = g^z / x^c$

a

c

z

Sigma Protocol for Diffie-Hellman tuples

Let G be a group of order q, with generators g and h

x=(g, h, u,v) Is a DH tuple if u=g^y, v=h^y

b⟵{0,1}
if b=0 then
T=(g, h, u=g^y, v=h^y)
else
T=(g, h, u=g^y, v=h^w) with y≠w

$\xrightarrow{T}$

Sigma Protocol for Diffie-Hellman tuples

y s.t. $u=g^y, v=h^y$

$x=(g, h, u, v)$

$\xrightarrow{A=g^r}$ $\xrightarrow{H=h^r}$

$\xleftarrow{c}$

$\xrightarrow{z=r+cy}$

Accept iff $g^z=Au^c$

and $h^z=Hv^c$

Sigma Protocol for Diffie-Hellman tuples

y s.t. $u=g^y, v=h^y$

$x=(g, h, u, v)$

$A=g^r$ $\longrightarrow$ $H=h^r$ $\longrightarrow$

$\longleftarrow$ c

$z=r+cy$ $\longrightarrow$

Accept iff $g^z=Au^c$

and $h^z=Hv^c$

$\mathcal{HVZK}_{sim}$

$c \Leftarrow Z_q$

$z \Leftarrow Z_q$

$A=g^z/u^c$

$H=h^z/v^c$

$a=(A,H)$ $\longrightarrow$

$\longleftarrow$ c

z $\longrightarrow$

HVZK

Sigma Protocol for Diffie-Hellman tuples

y s.t. $u=g^y, v=h^y$

$x=(g, h, u, v)$

$A=g^r$ $\longrightarrow$ $H=h^r$ $\longrightarrow$

$\longleftarrow$ c

$z=r+cy$ $\longrightarrow$

Accept iff $g^z=Au^c$

and $h^z=Hv^c$

Special-soundness

Exactly the same as the one for the Dlog protocol

OR-Composition

$\Sigma_0=(P_{\Sigma_0},V_{\Sigma_0})$

x_0 or x_1

$\Sigma_1=(P_{\Sigma_1},V_{\Sigma_1})$

a_0 →

c_0 ←

z_0 →

$\mathcal{HVZK}^0{}_{sim}(x_0) \longrightarrow a_0,c_0,z_0$

$\mathcal{HVZK}^1{}_{sim}(x_1) \longrightarrow a_1,c_1,z_1$

a_1 →

c_1 ←

z_1 →

w_0

$\mathcal{HVZK}^1{}_{sim}(x_1) \longrightarrow a_1,c_1,z_1$

$a_0 \longleftarrow P_{\Sigma_0}(x_0,w_0)$

a_0 → a_1 →

c ←

$c_0 \longleftarrow c \oplus c_1$

$z_0 \longleftarrow P_{\Sigma_0}(x_0,w_0,c_0)$

c_0, z_0 → c_1, z_1 →

$V_{\Sigma_0}(x_0,a_0,c_0,z_0)=1$

and

$V_{\Sigma_1}(x_1,a_1,c_1,z_1)=1$

and

$c=c_0 \oplus c_1$

OR-Composition

x_0 or x_1

Special Soundness

a_0 $\quad$ a_1

c $\quad$ c'

c_0, z_0 $\quad$ c_1, z_1 $\quad$ c'_0, z'_0 $\quad$ c'_1, z'_1

$V_{\Sigma_0}(x_0,a_0,c_0,z_0)=1$ $\quad$ $V_{\Sigma_0}(x_0,a_0,c'_0,z'_0)=1$

and $\quad$ and

$V_{\Sigma_1}(x_1,a_1,c_1,z_1)=1$ $\quad$ $V_{\Sigma_1}(x_1,a_1,c'_1,z'_1)=1$

and $\quad$ and

$c=c_0\oplus c_1$ $\quad$ $c'=c'_0\oplus c'_1$

$c \neq c'$

$c_0 \neq c'_0$

or

$c_1 \neq c'_1$

e.g. $c_0 \neq c'_0$

by s-soundness of Σ_0

w_0

Michele Ciampi The University of Edinburgh

AND-Composition

$\Sigma_0 = (P_{\Sigma_0}, V_{\Sigma_0})$

x_0 AND x_1

$\Sigma_1 = (P_{\Sigma_1}, V_{\Sigma_1})$

Σ_0: $\xrightarrow{a_0}$, $\xleftarrow{c_0}$, $\xrightarrow{z_0}$

$\mathcal{HVZK}^0{}_{sim}(x_0) \longrightarrow a_0, c_0, z_0$

$\mathcal{HVZK}^1{}_{sim}(x_1) \longrightarrow a_1, c_1, z_1$

Σ_1: $\xrightarrow{a_1}$, $\xleftarrow{c_1}$, $\xrightarrow{z_1}$

w_0, w_1

$a_0 \longleftarrow P_{\Sigma_0}(x_0, w_0)$

$a_1 \longleftarrow P_{\Sigma_1}(x_1, w_1)$

$\xrightarrow{a_0} \xrightarrow{a_1}$

$\xleftarrow{c}$

$z_0 \longleftarrow P_{\Sigma_0}(x_0, w_0, c)$

$z_1 \longleftarrow P_{\Sigma_0}(x_1, w_1, c)$

$\xrightarrow{z_0} \xrightarrow{z_1}$

$V_{\Sigma_0}(x_0, a_0, c, z_0) = 1$

and

$V_{\Sigma_1}(x_1, a_1, c, z_1) = 1$

AND-Composition

x_0 AND x_1

Special Soundness

$a_0 \longleftarrow P_{\Sigma_0}(x_0, w_0)$

$a_1 \longleftarrow P_{\Sigma_1}(x_1, w_1)$

$\xrightarrow{a_0}$ $\xrightarrow{a_1}$

$\xleftarrow{c}$ $\xleftarrow{c'}$

$z_0 \longleftarrow P_{\Sigma_0}(x_0, w_0, c)$

$z_1 \longleftarrow P_{\Sigma_0}(x_1, w_1, c)$

$\xrightarrow{z_0}$ $\xrightarrow{z_1}$ $\xrightarrow{z'_0}$ $\xrightarrow{z'_1}$

$V_{\Sigma_0}(x_0,a_0,c,z_0)=1$ $V_{\Sigma_0}(x_0,a_0,c',z'_0)=1$

and and

$V_{\Sigma_1}(x_1,a_1,c,z_1)=1$ $V_{\Sigma_1}(x_1,a_1,c',z'_1)=1$

$c \neq c'$
and
s-soundness of
Σ_0 and Σ_1

$\Rightarrow$ w_0, w_1

Michele Ciampi The University of Edinburgh

Commitments from Sigma-Protocols

Commitment scheme

m → Commit(m) → **com, dec**

com, m, **dec** → Decommit(**com,** m**, dec**) → **1/0**

- Hiding
- Binding
  ∄ **dec'**, m', with m≠m' s.t.
  Decommit(**com,** m**, dec**)=1 and
  Decommit(**com,** m'**, dec'**)=1

Instance-dependent commitment scheme
NP-Language L

x, m → Commit(**x**,m) → **com,dec**

x, **com**, m, **dec** → Decommit(**x**, **com,** m**, dec**) → **1/0**

- if **x** ∈ L Hiding
- If **x** ∉ L Binding
  ∄ **dec'**, m', with m≠m' s.t.
  Decommit(**x**, **com,** m**, dec**)=1 and
  Decommit(**x**, **com,** m'**, dec'**)=1

Commitments from Sigma-Protocols

$\Sigma=(P_\Sigma,V_\Sigma)$

$P \xrightarrow{a} V$, $V \xrightarrow{c} P$, $P \xrightarrow{z} V$

$\mathcal{SHVZK}_{sim}(\mathbf{x},c) \longrightarrow a, z$

Inputs: $\mathbf{x}$, m

$\mathcal{SHVZK}_{sim}(\mathbf{x},m) \longrightarrow a, z$

com $\longleftarrow$ a

dec $\longleftarrow$ z

Output: **com, dec**

Inputs: $\mathbf{x}$, **com**, m, **dec**

$V_\Sigma(\mathbf{x}, \mathbf{com}, m, \mathbf{dec}) \longrightarrow \mathbf{b}$

Output: **b**

Binding (x ∉ L)

m'≠m

$V_\Sigma(\mathbf{x}, \mathbf{com}, m, \mathbf{dec}) \longrightarrow 1$

$V_\Sigma(\mathbf{x}, \mathbf{com}, m', \mathbf{dec'}) \longrightarrow 1$

s-soundness of Σ $\Longrightarrow$ w: witness for $\mathbf{x}$

Michele Ciampi The University of Edinburgh

Commitments from Sigma-Protocols

Hiding $(x \in L)$

$b \leftarrow \{0,1\}$

$\mathbf{x}$ $\quad$ m_b

$\mathcal{SHVZK}_{sim}(\mathbf{x}, m_b) \longrightarrow a, z$

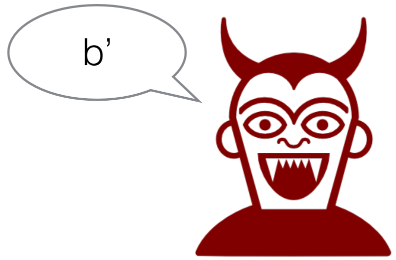
com $\longleftarrow a$

dec $\longleftarrow z$

com, dec

m_0, m_1

com



By contradiction b=b’

$a_0 =$ **com** $\equiv$ $a \longleftarrow P_\Sigma(x, w)$ $\equiv$ $a_1 =$ **com**

$\mathcal{SHVZK}_{sim}(\mathbf{x}, m_0) \longrightarrow$ $\quad$ $\longleftarrow \mathcal{SHVZK}_{sim}(\mathbf{x}, m_1)$

z_0 $\quad$ $z \longleftarrow P_\Sigma(x, w, m_0)$ $\quad$ z_1

Conclusions

- Sigma protocols exist for a variety of NP languages
- Practical efficiency
- Building blocks for efficient zero-knowledge protocols
    - Interactive
    - Non-interactive (Fiat-Shamir Transform)

De Componendis Cifris

https:/www.decifris.it

Reference: On Sigma-Protocols. Ivan Damgaard. https://www.cs.au.dk/~ivan/Sigma.pdf