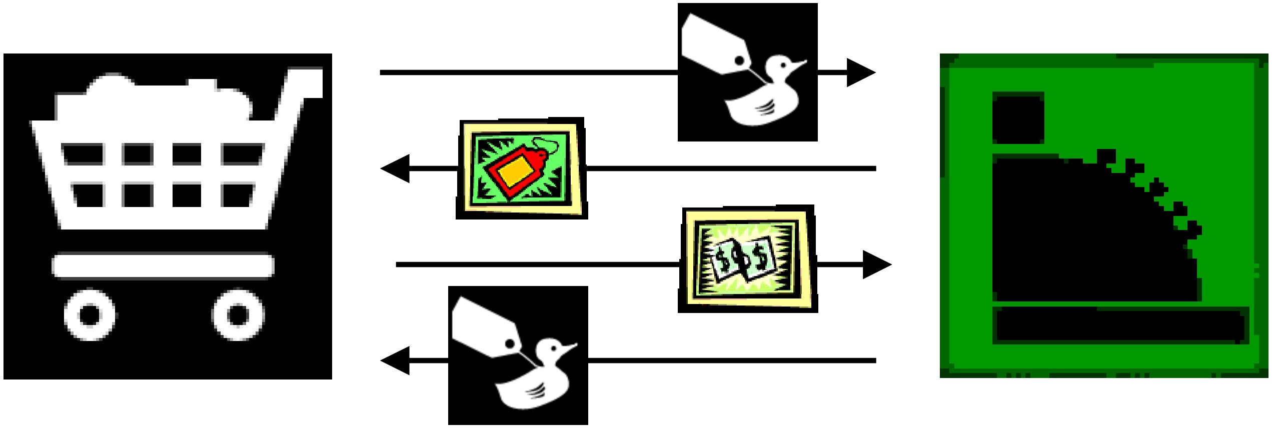
Design patterns in protocol derivation

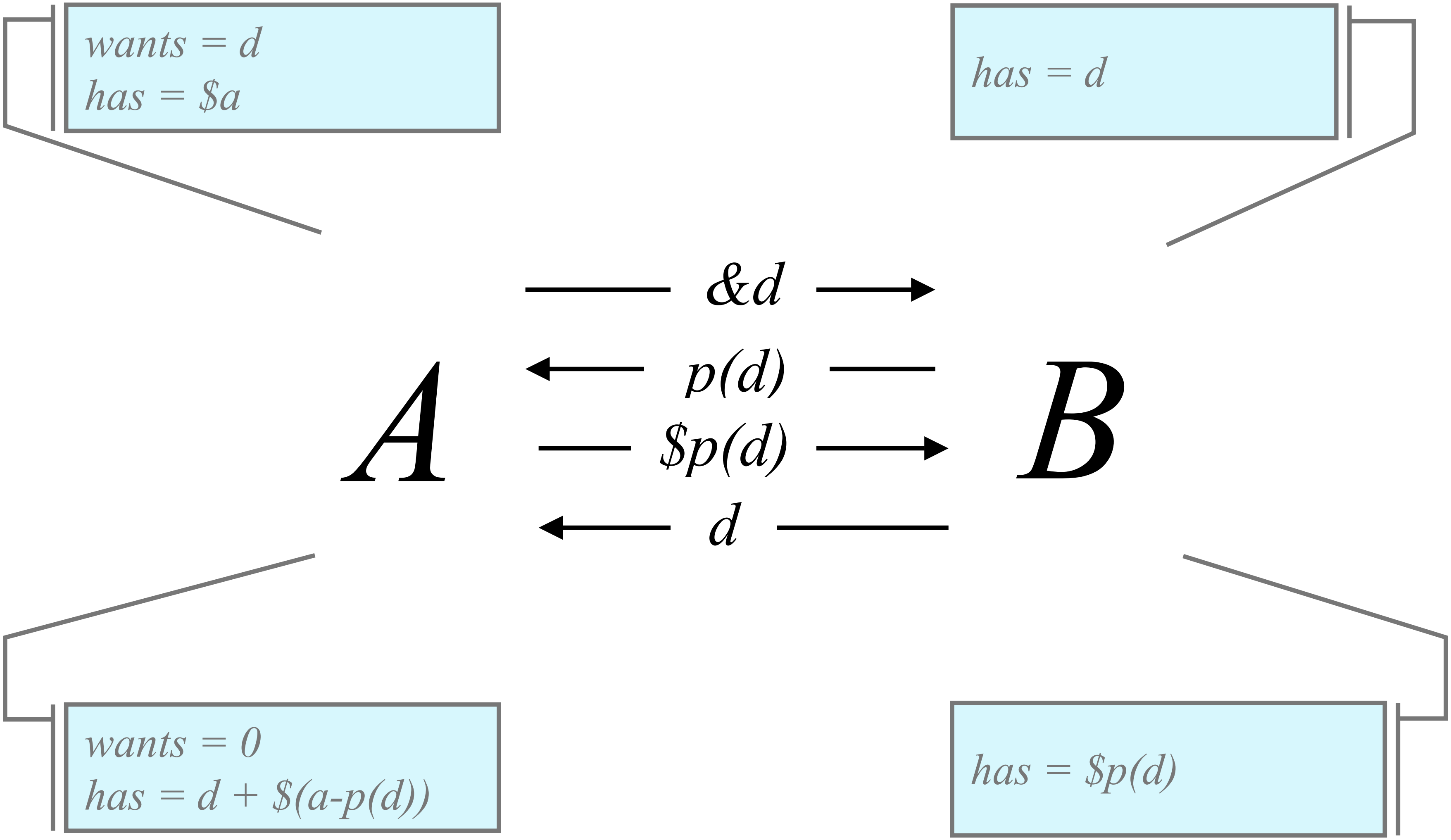
Dusko Pavlovic
Kestrel Institute

March, 2003

What is a protocol?



What is a protocol?



wants = d
has = $a

has = d

&d →

← *p(d)*

$p(d) →

← *d*

A

B

wants = 0
has = d + $(a-p(d))

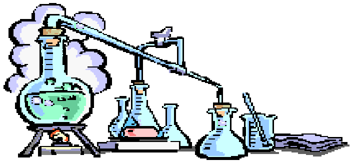
has = $p(d)

What is a protocol?

- “language for dialog”

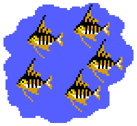
  - rules of social interaction

  - politics, law, market
  - lab protocols, experiment design



  - “language games”

  - distributed programs



What is a protocol?

- distributed computation
  - – computation traces: $\mathrm{L} \subseteq A^*$
  - – protocol: $\mathrm{P} \subseteq (A_1 + A_2 + \ldots + A_n)^*$
    - » *Characterize distributed grammars, distributed Church's thesis, distributed complexity classes!*
- distributed program
  - – computation = game between System and Environment
  - – program = strategy for System
  - – protocol = strategy for the team of System
    - » concurrency
    - » locality, imperfect information
      - experiment design: devising information channels

What is a security property?

- syntactically
  - more special than safety/liveness
- semantically
  - more general than safety/liveness
    - local state (imperfect information)
    - experiments (information channels)
    - not inductive, but coinductive: circular, impredicative
    - not compositional

equilibria,
language games

Plan

- develop tools for distributed programming
  - techniques of interaction design
    - drama
    - music
  - based on libraries of reusable
    - components
    - connectors
    - design patterns

Idea

Protocol derivation

- components
- refinements
- transformations

Proof derivation

- axioms
- proof rules
- proof transformations

design patterns

Approach

Security Engineering

is a part of

Software Engineering

Outline: derivation steps

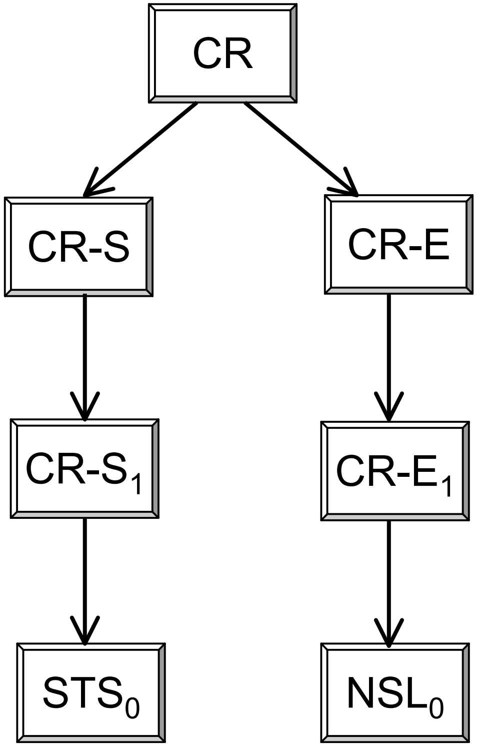
1. Authenticated DH
   - $CR \rightarrow STS$
2. Identity and DoS protection
   - $STS \rightarrow JFK$
3. DH refinements
   - $KA \rightarrow MQV$
4. Combine 2. and 3.
   - $MQV \rightarrow MQV_{+}$

Papers

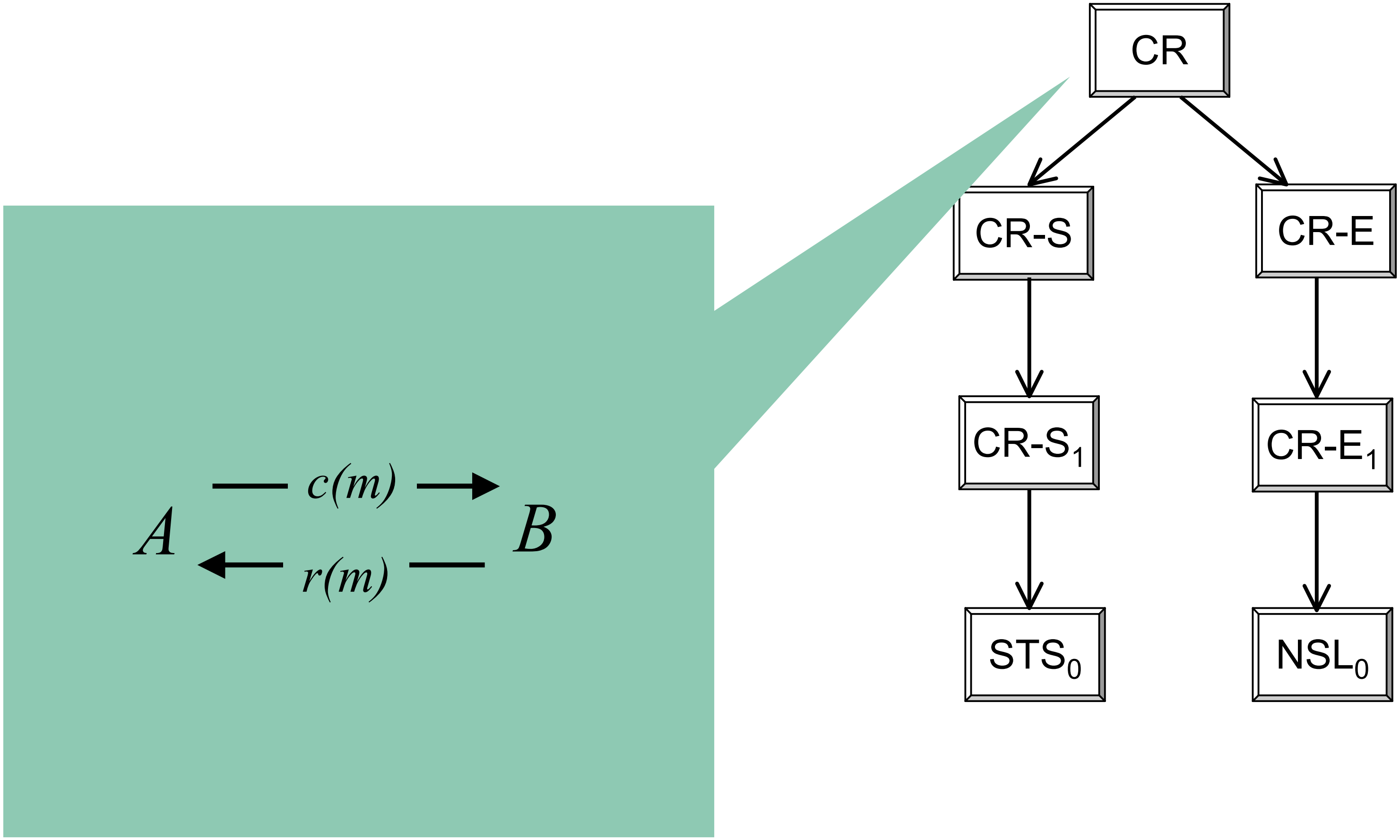
- Derivation of JFK
  - with A. Datta and J. Mitchell
- A derivation system for security protocols and its logical formalization
  - with A. Datta, A. Derek and J. Mitchell
- Design patterns in protocol derivation
  - in preparation

http://www.kestrel.edu/users/pavlovic/

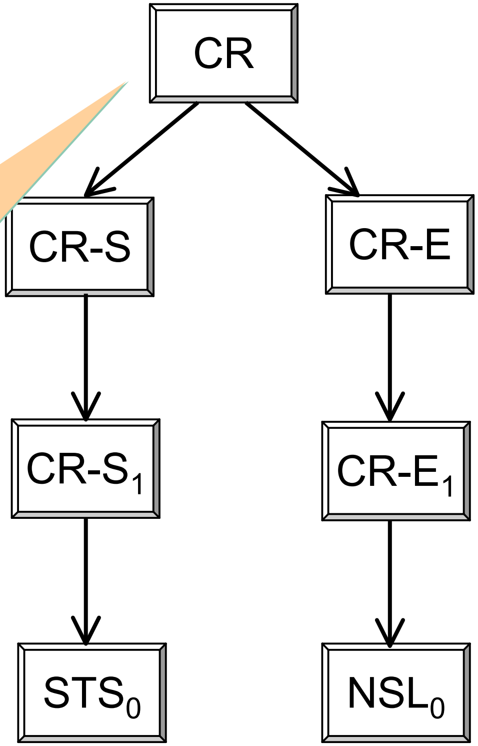
Basic challenge-response



Basic challenge-response



Basic challenge-response



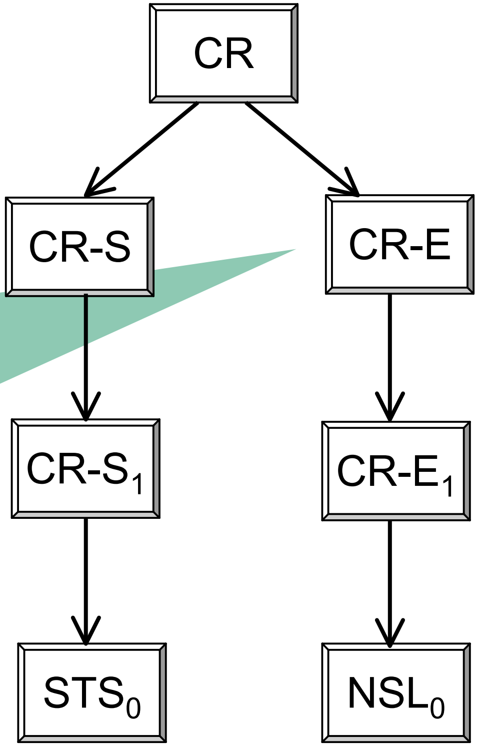
[A and B know each other.]

A: *"B was alive after m was generated."*

B: *"X wants to talk, and knows that I am alive."*

Basic challenge-response

$$\begin{tikzcd} A \arrow[r, shift left, "E_B(m)"] & B \arrow[l, shift left, "m"] \end{tikzcd}$$

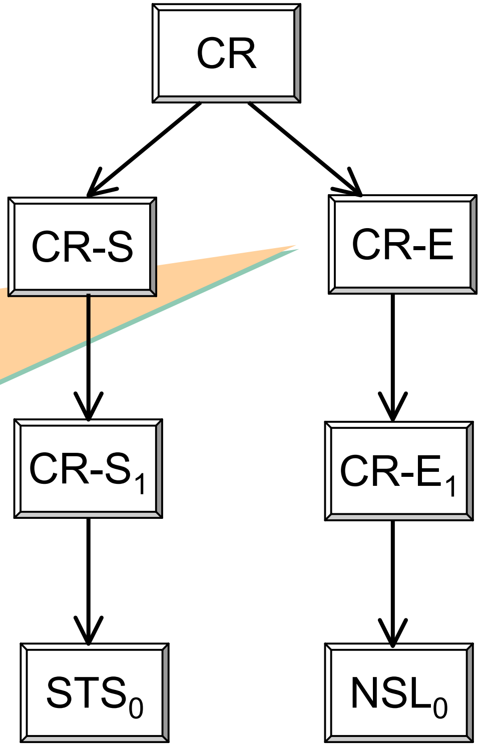


Basic challenge-response

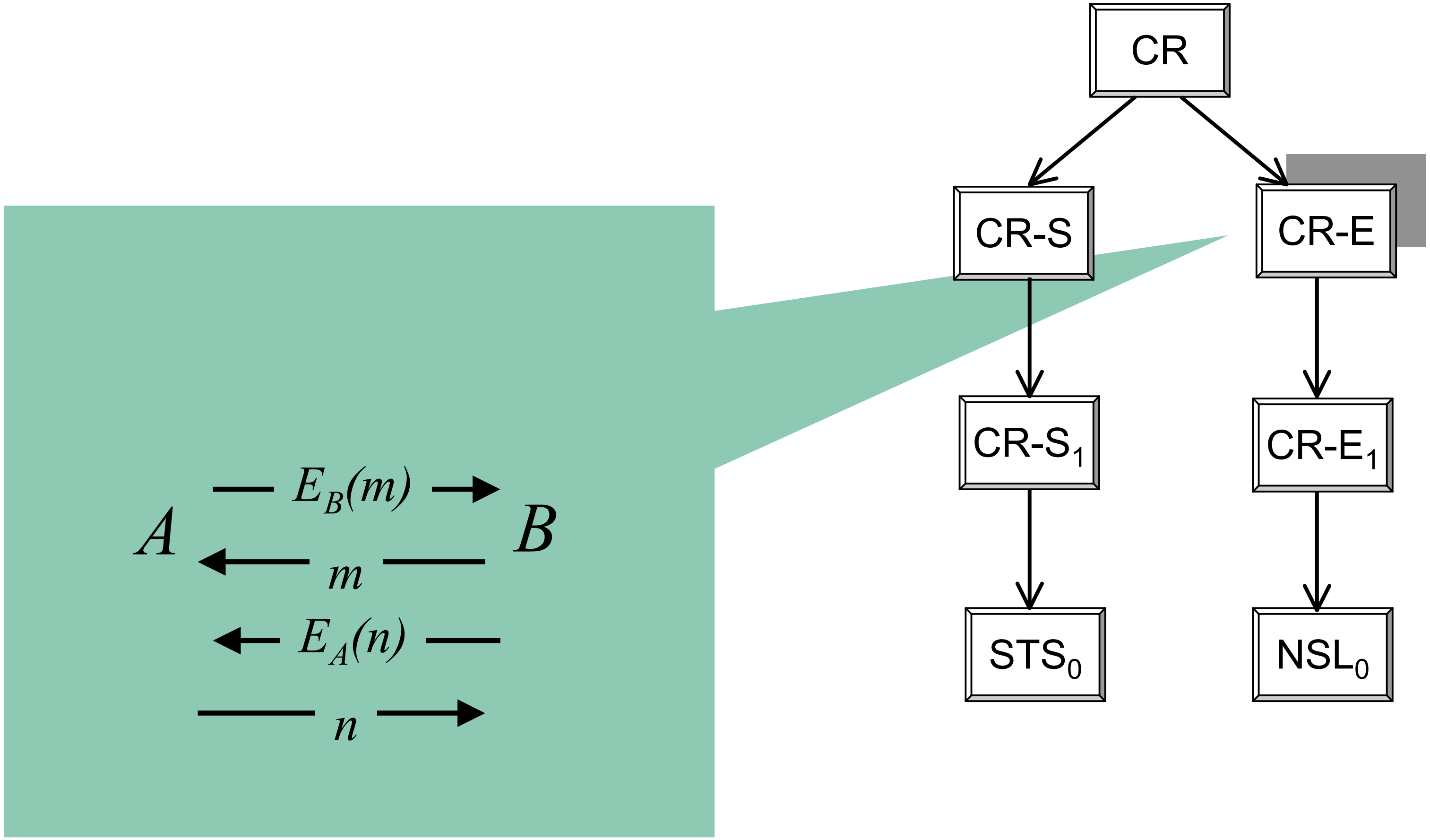
[A and B know each other.]

A: *“B was alive after m was generated.”*

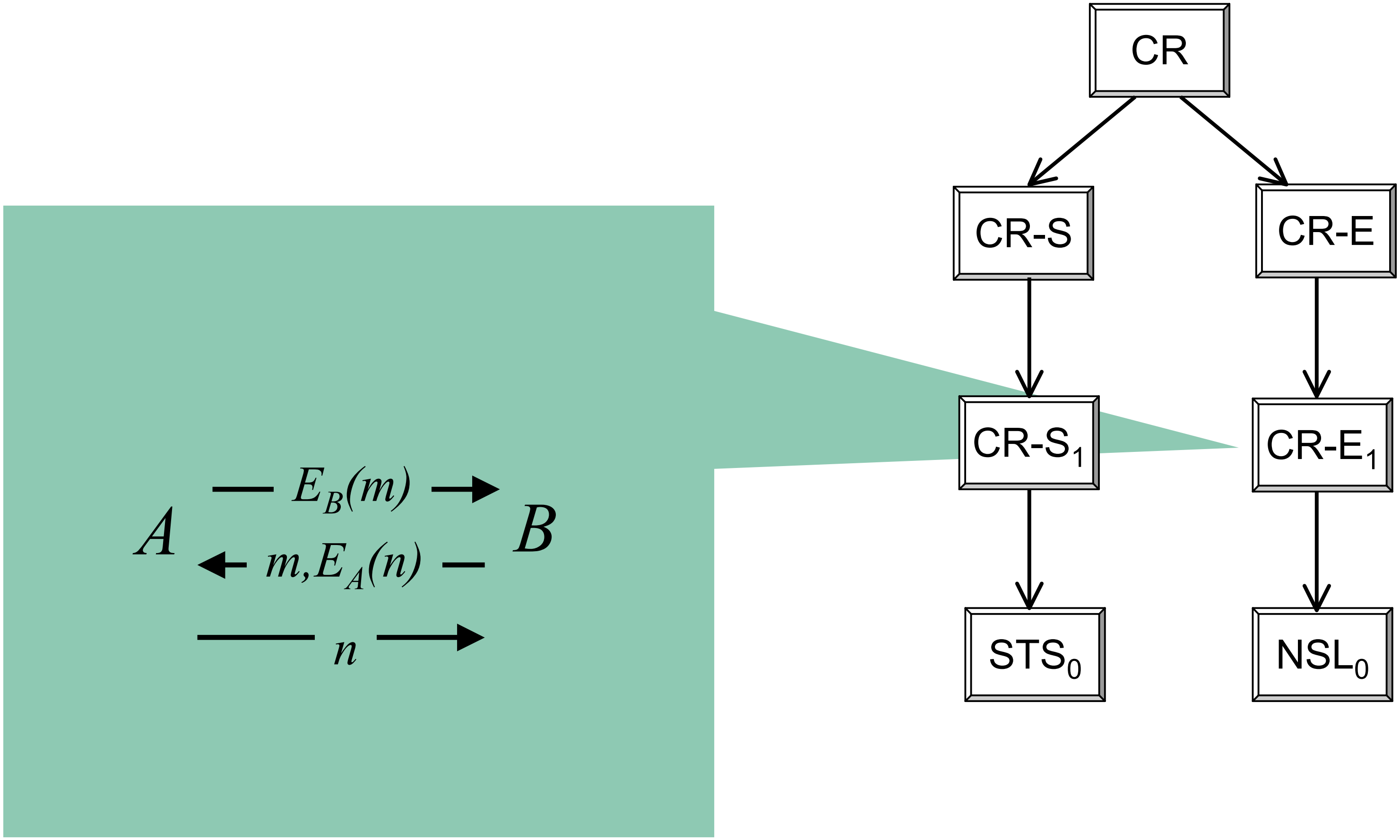
B: *“X wants to talk, and knows that I am alive.”*



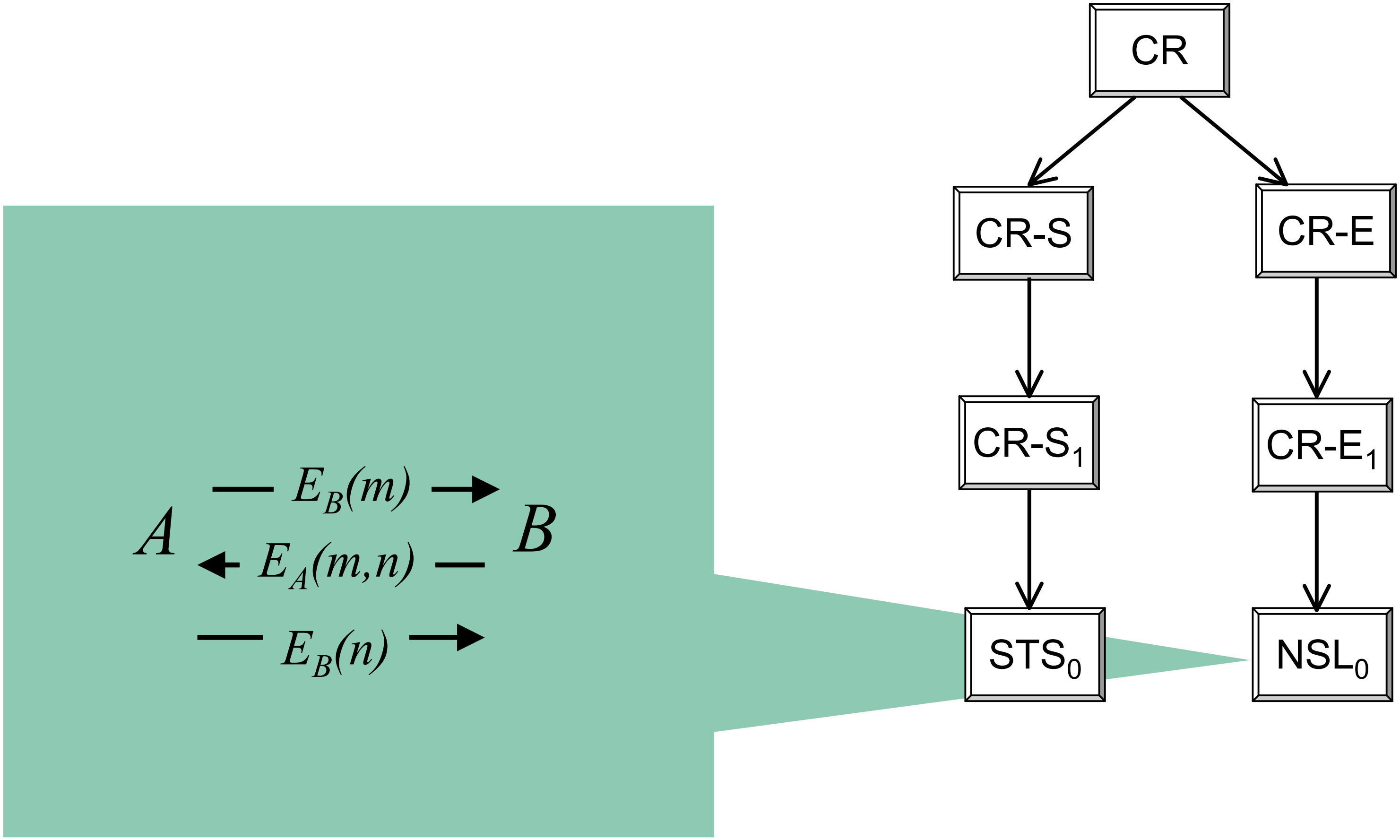
Basic challenge-response



Basic challenge-response

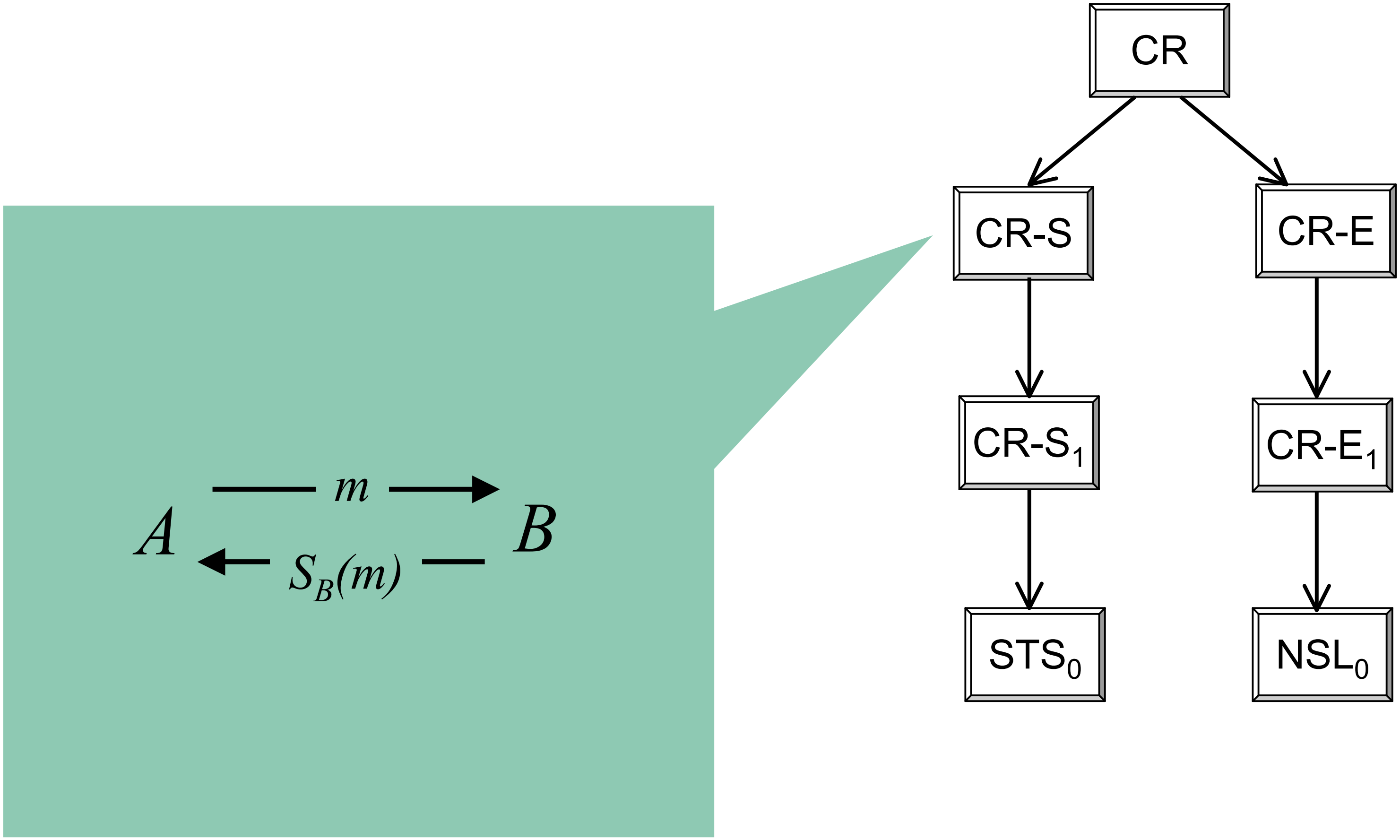


Basic challenge-response

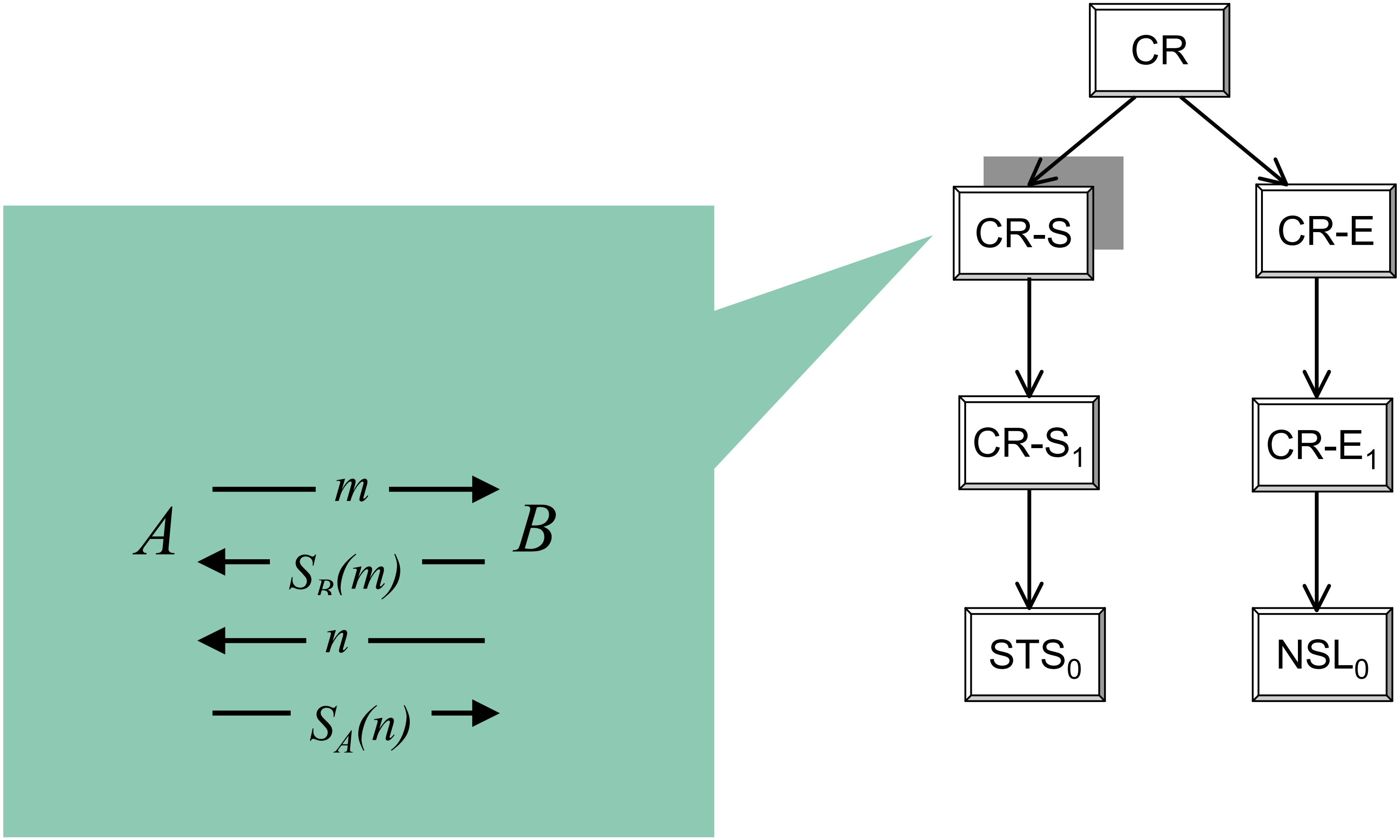


$$A \xrightarrow{E_B(m)} B$$
$$A \xleftarrow{E_A(m,n)} B$$
$$A \xrightarrow{E_B(n)} B$$

Basic challenge-response



Basic challenge-response



CR

CR-S

CR-E

CR-S$_1$

CR-E$_1$

STS$_0$

NSL$_0$

A $\xrightarrow{m}$ B

A $\xleftarrow{S_B(m)}$ B

A $\xleftarrow{n}$ B

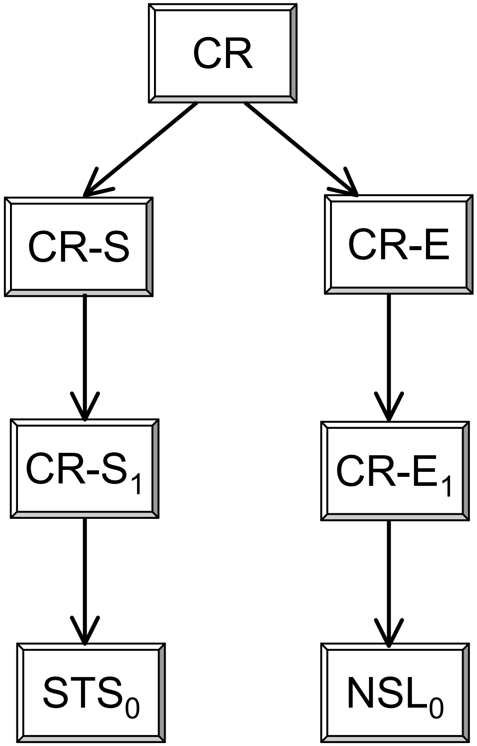
A $\xrightarrow{S_A(n)}$ B

Basic challenge-response

$$A \xrightarrow{\quad m \quad} B$$

$$A \xleftarrow{\quad S_B(m), n \quad} B$$

$$A \xrightarrow{\quad S_A(n) \quad} B$$

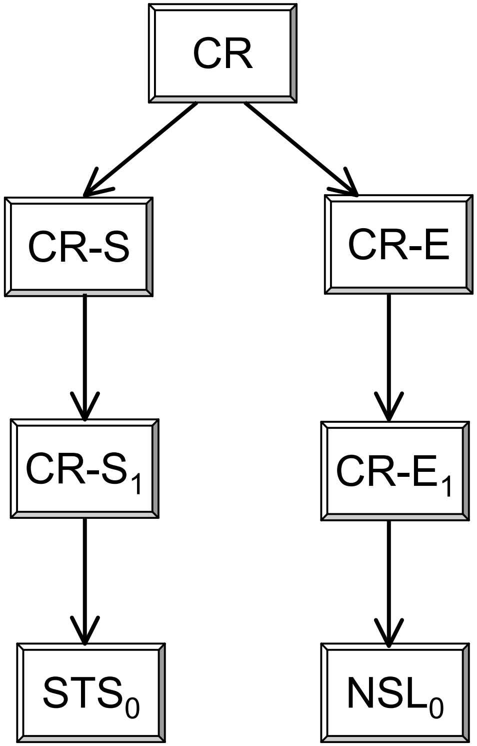


Basic challenge-response

$$A \xrightarrow{\quad m \quad} B$$

$$A \xleftarrow{\quad S_B(m),n,n \quad} B$$

$$A \xrightarrow{\quad S_A(n),m \quad} B$$

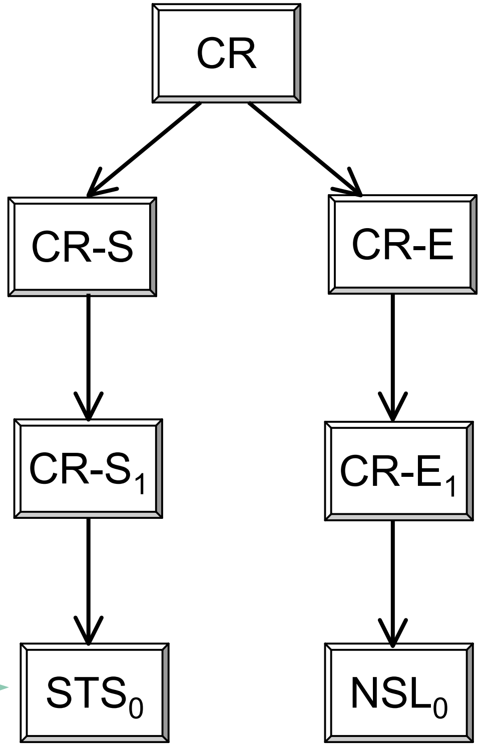


Basic challenge-response

$$A \xrightarrow{\quad m \quad} B$$

$$A \xleftarrow{\quad S_B(m,n),n \quad} B$$

$$A \xrightarrow{\quad S_A(n,m) \quad} B$$

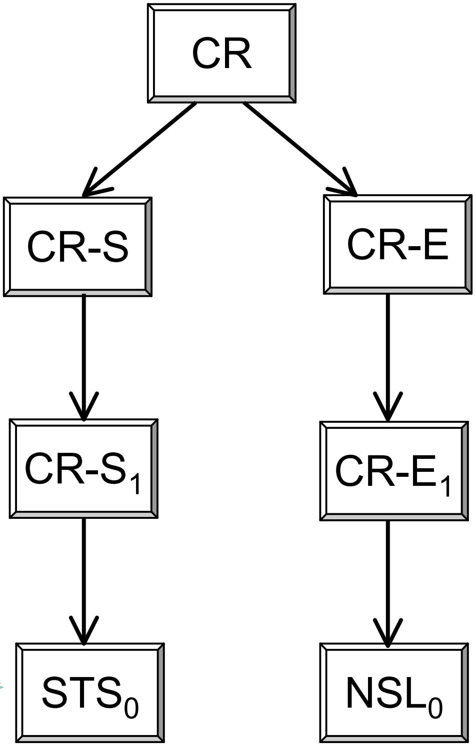


Basic challenge-response

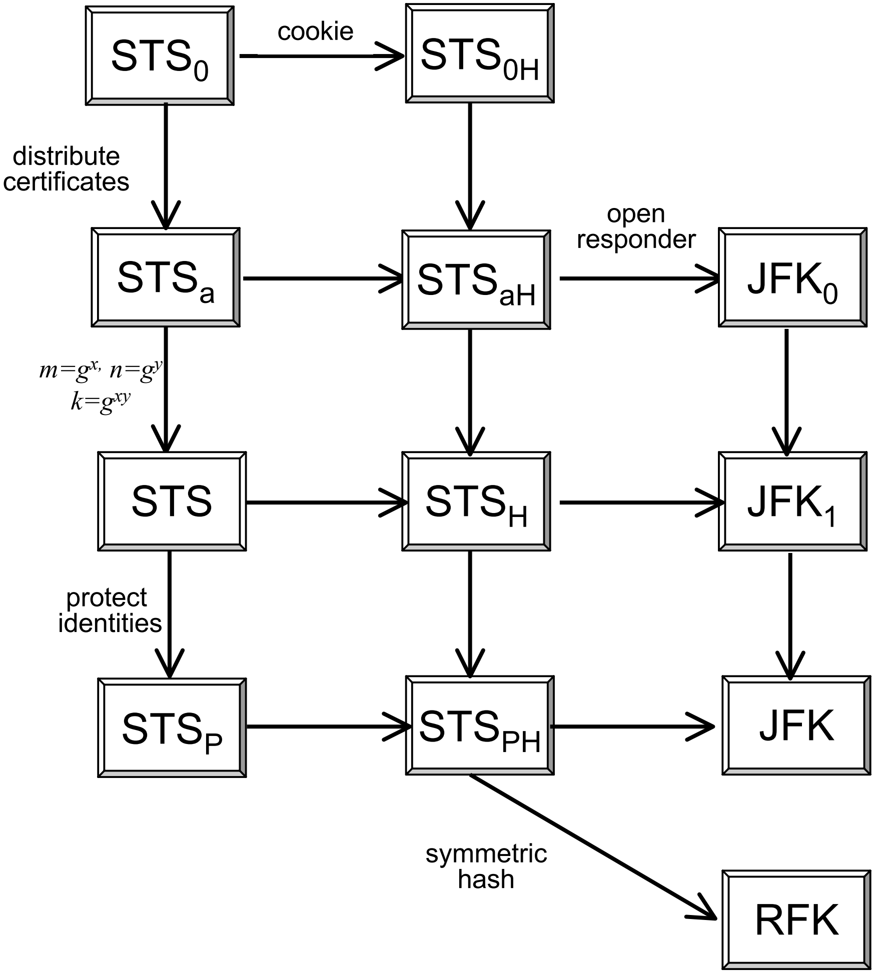
[A and B know each other.]

A: *“B accepts session, was alive after m*
was generated and knows that
I am alive after n.”

B: *“A wants to talk, was alive after n*
was generated and knows that
I am alive after m.”



STS family



STS_0

cookie

STS_{0H}

distribute certificates

STS_a

STS_{aH}

open responder

JFK_0

$m=g^x, n=g^y$

$k=g^{xy}$

STS

STS_H

JFK_1

protect identities

STS_P

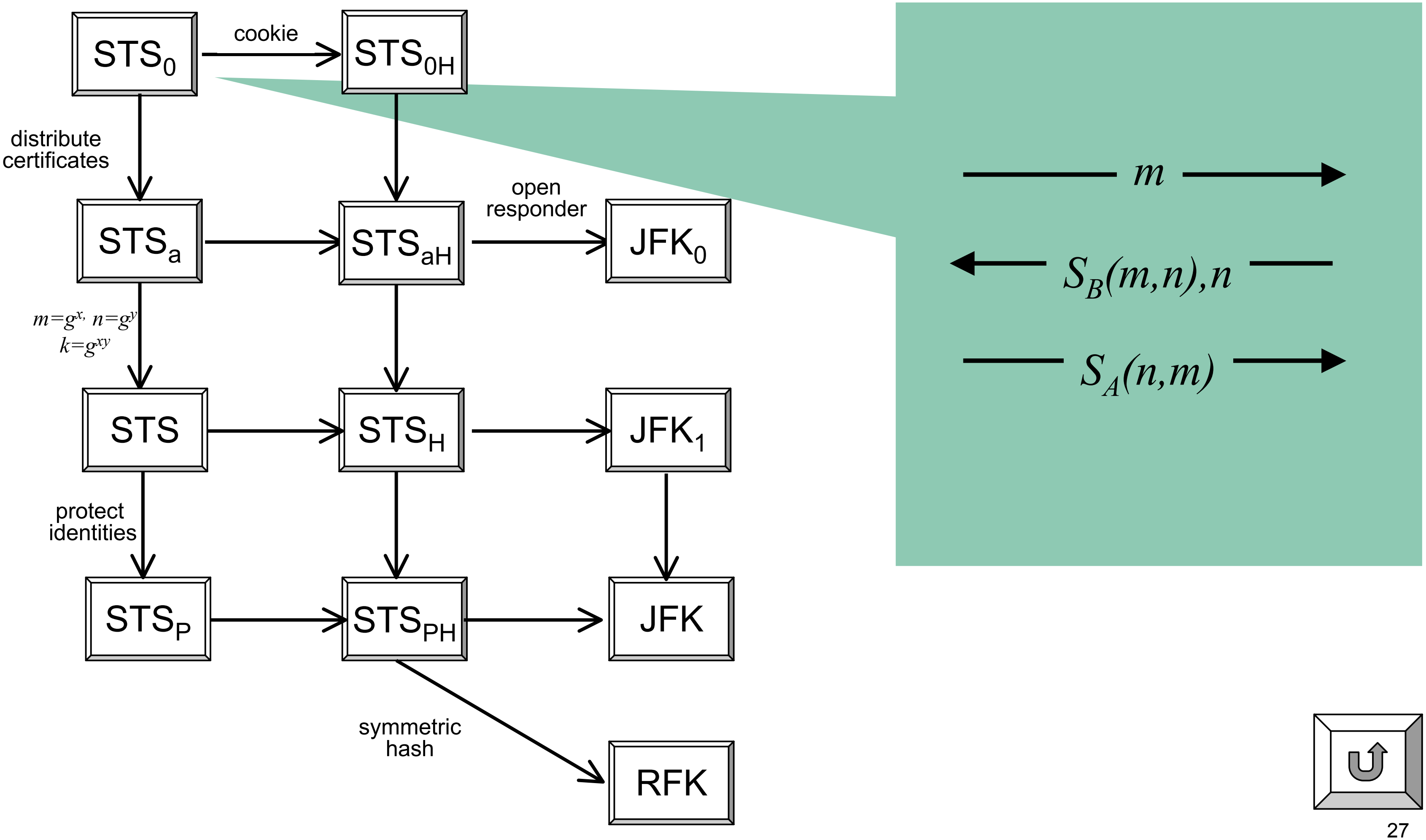
STS_{PH}

JFK

symmetric hash

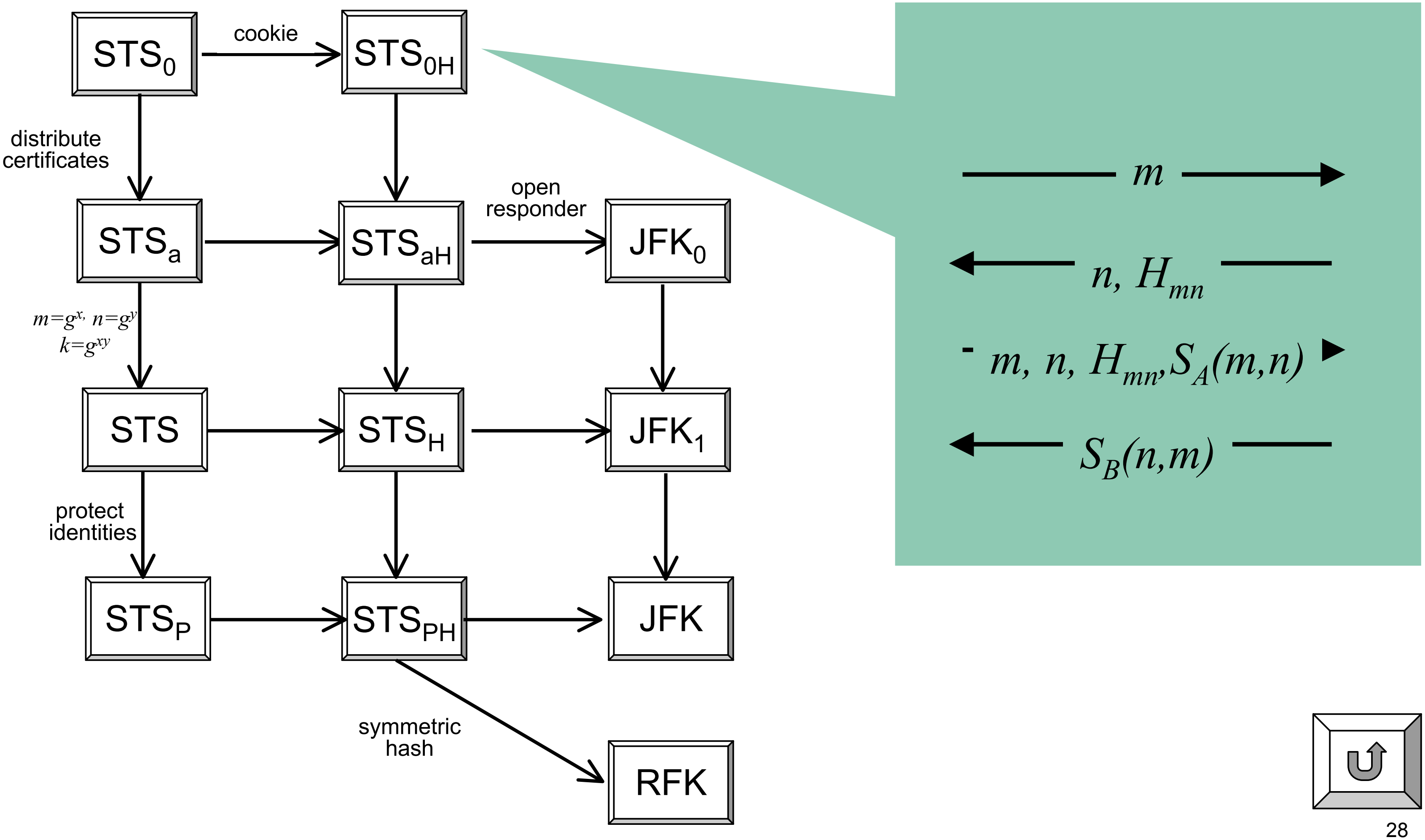
RFK

STS family

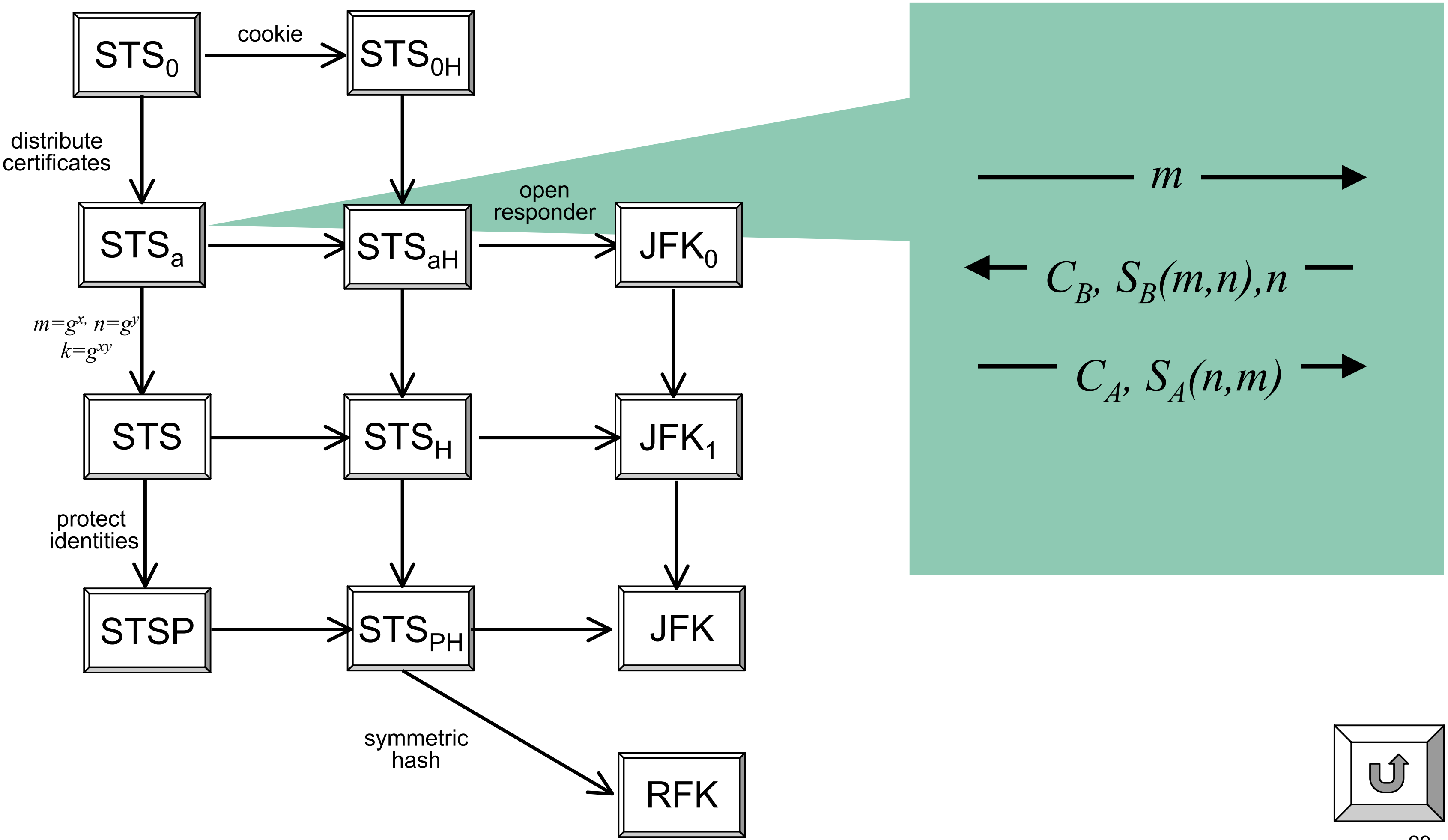


STS_0
cookie
STS_{0H}
distribute certificates
STS_a
STS_{aH}
open responder
JFK_0
$m=g^x, n=g^y$
$k=g^{xy}$
STS
STS_H
JFK_1
protect identities
STS_P
STS_{PH}
JFK
symmetric hash
RFK
m
$S_B(m,n),n$
$S_A(n,m)$

STS family

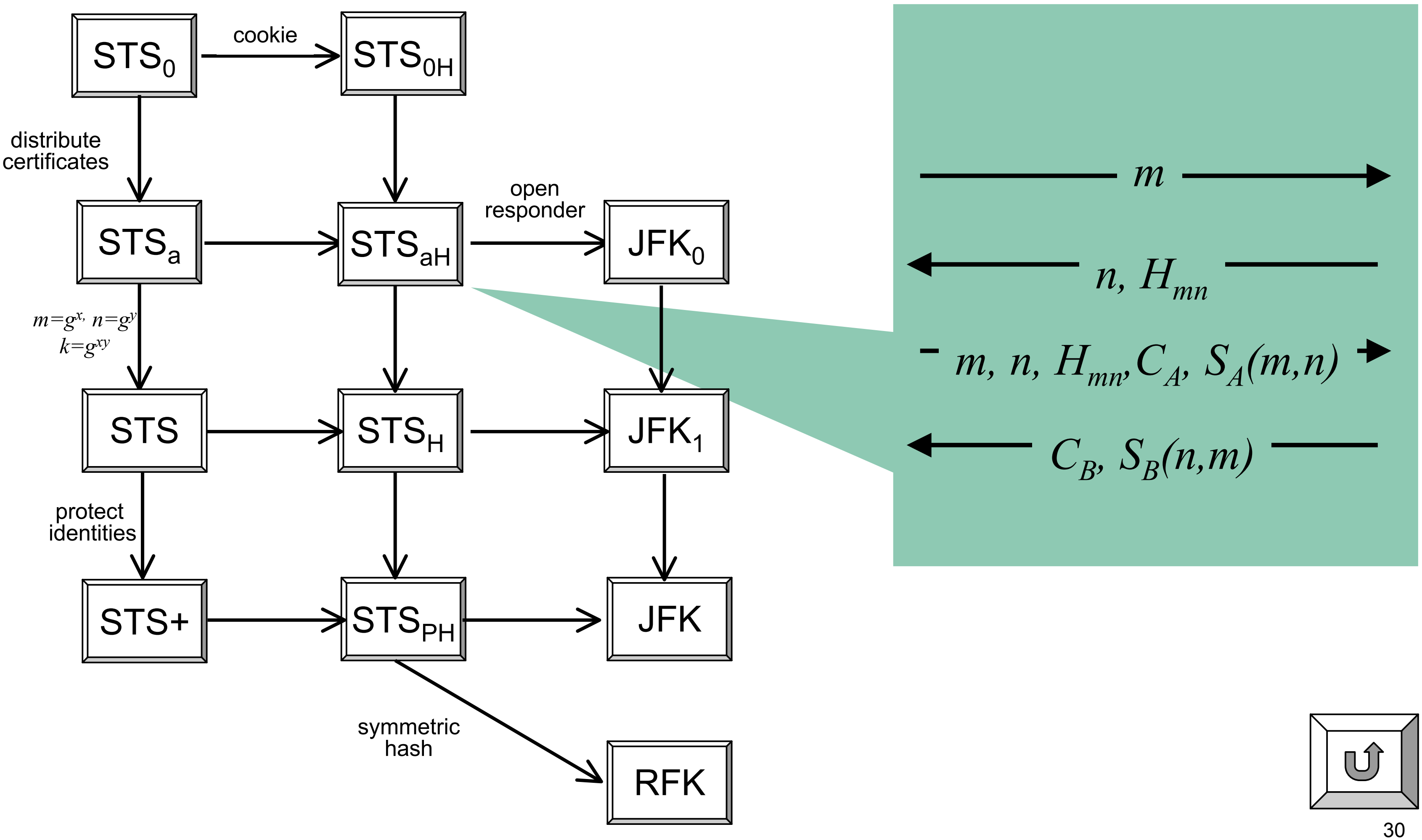

STS_0
cookie
STS_{0H}
distribute certificates
STS_a
STS_{aH}
open responder
JFK_0
$m=g^x,\ n=g^y$
$k=g^{xy}$
STS
STS_H
JFK_1
protect identities
STS_P
STS_{PH}
JFK
symmetric hash
RFK
m
$n,\ H_{mn}$
$m,\ n,\ H_{mn},S_A(m,n)$
$S_B(n,m)$

STS family



STS$_0$
cookie
STS$_{0H}$
distribute certificates
STS$_a$
open responder
STS$_{aH}$
JFK$_0$
$m=g^x$, $n=g^y$
$k=g^{xy}$
STS
STS$_H$
JFK$_1$
protect identities
STSP
STS$_{PH}$
JFK
symmetric hash
RFK
m
C_B, $S_B(m,n),n$
C_A, $S_A(n,m)$

STS family



STS_0 — cookie → STS_{0H}

STS_0 — distribute certificates → STS_a

STS_{0H} → STS_{aH}

STS_a → STS_{aH} — open responder → JFK_0

STS_a — $m=g^x$, $n=g^y$, $k=g^{xy}$ → STS

STS_{aH} → STS_H

JFK_0 → JFK_1

STS → STS_H → JFK_1

STS — protect identities → STS+

STS_H → STS_{PH}

JFK_1 → JFK

STS+ → STS_{PH} → JFK

STS_{PH} — symmetric hash → RFK

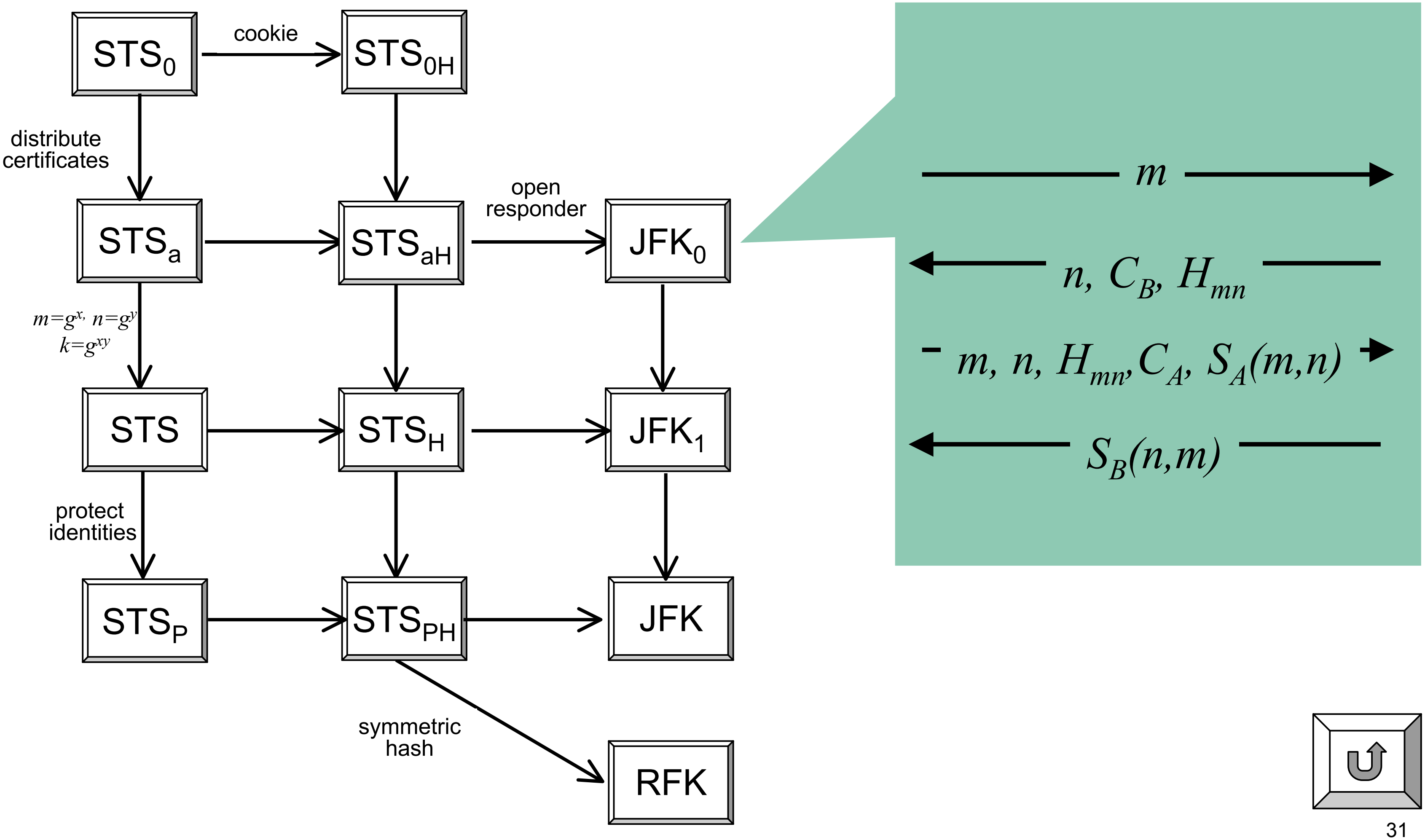
$$\xrightarrow{\quad m \quad}$$

$$\xleftarrow{\quad n,\ H_{mn} \quad}$$

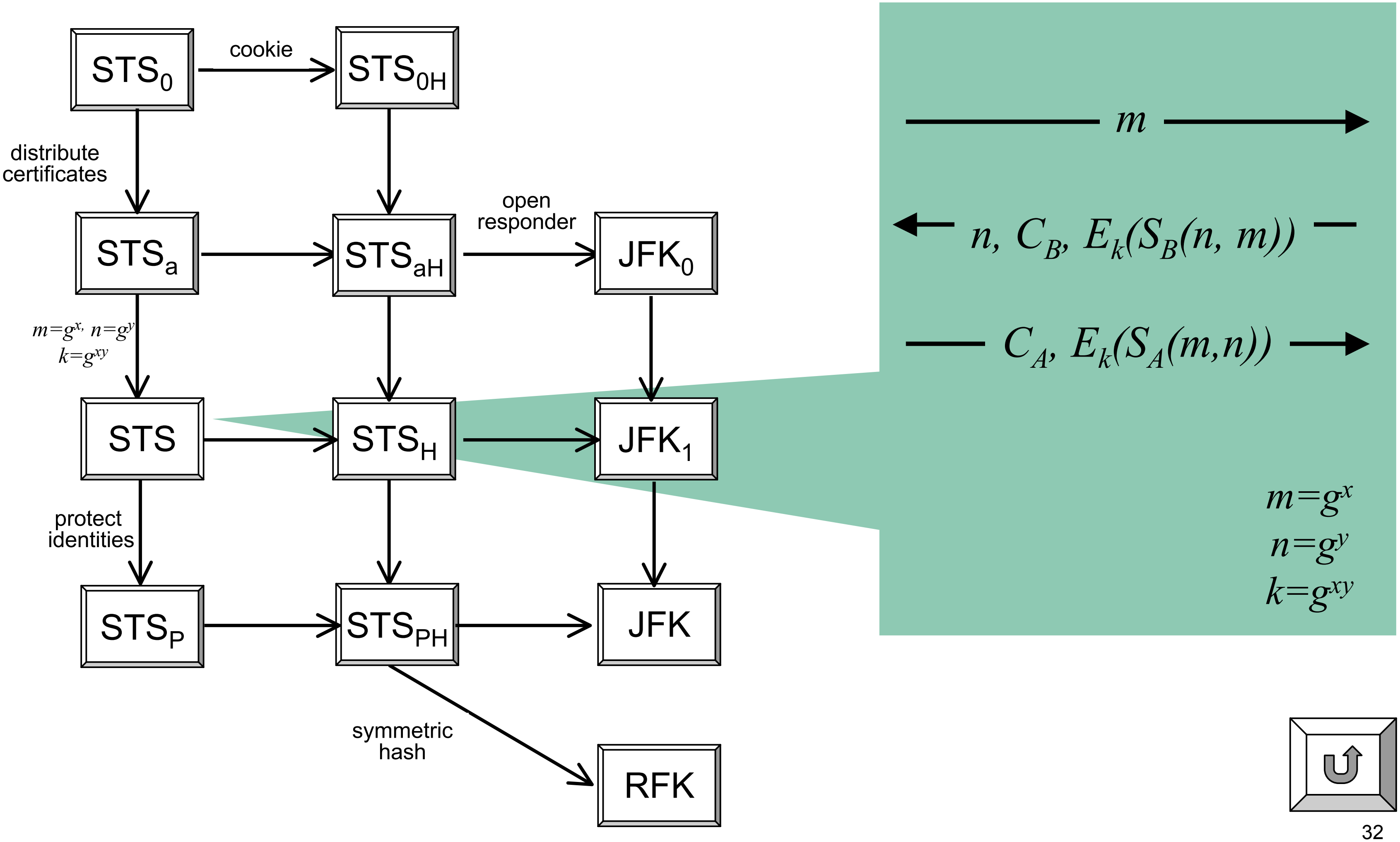
$$\xrightarrow{\quad m,\ n,\ H_{mn},C_A,\ S_A(m,n) \quad}$$

$$\xleftarrow{\quad C_B,\ S_B(n,m) \quad}$$

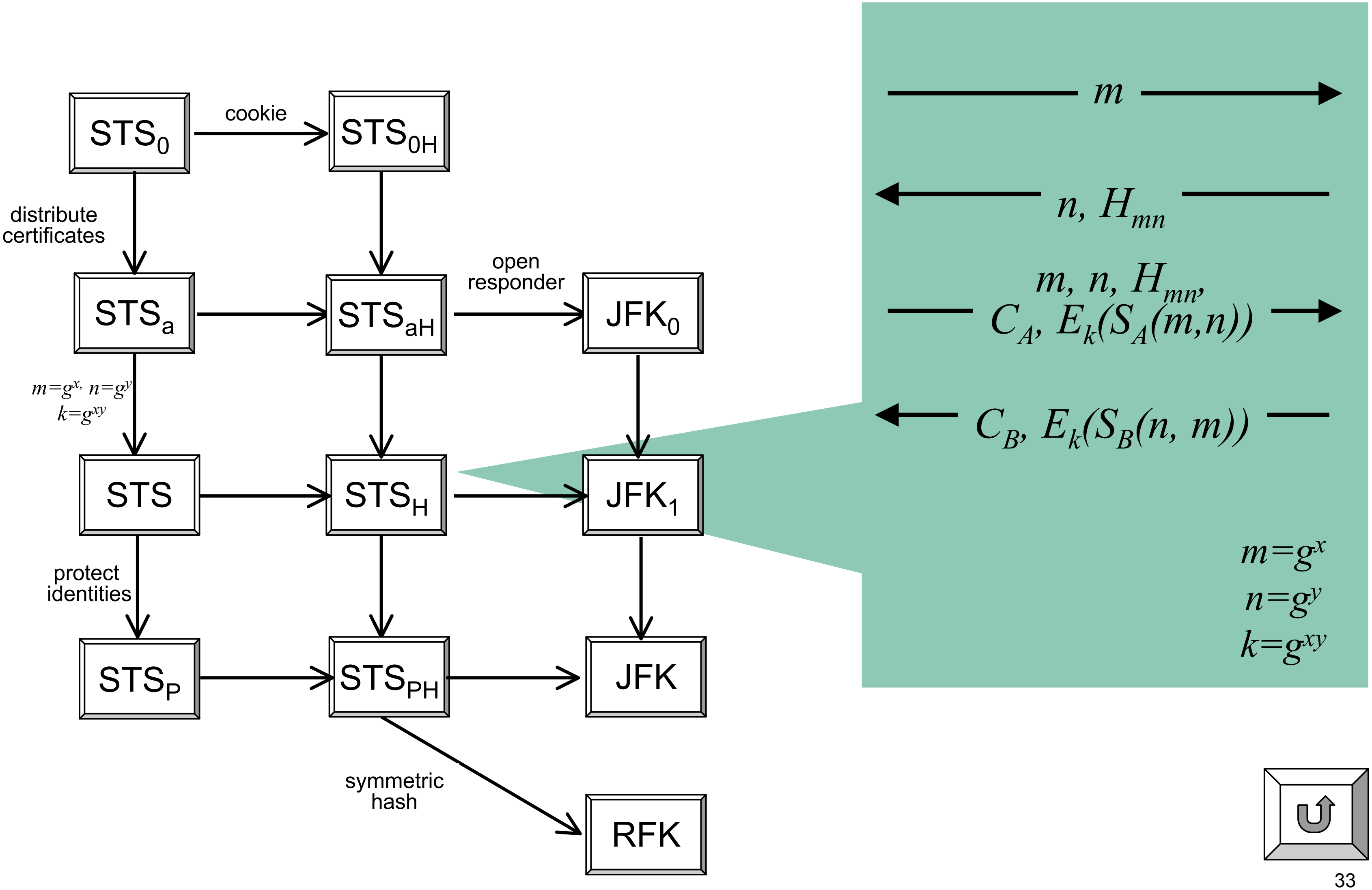
STS family


STS_0
cookie
STS_{0H}
distribute certificates
STS_a
STS_{aH}
open responder
JFK_0
$m=g^x, n=g^y$
$k=g^{xy}$
STS
STS_H
JFK_1
protect identities
STS_P
STS_{PH}
JFK
symmetric hash
RFK
m
n, C_B, H_{mn}
$m, n, H_{mn}, C_A, S_A(m,n)$
$S_B(n,m)$

STS family


STS$_0$
cookie
STS$_{0H}$
distribute certificates
STS$_a$
STS$_{aH}$
open responder
JFK$_0$
$m=g^x, n=g^y$
$k=g^{xy}$
STS
STS$_H$
JFK$_1$
protect identities
STS$_P$
STS$_{PH}$
JFK
symmetric hash
RFK
m
$n, C_B, E_k(S_B(n, m))$
$C_A, E_k(S_A(m,n))$
$m=g^x$
$n=g^y$
$k=g^{xy}$

STS family



STS_0 cookie STS_{0H}

distribute certificates

STS_a STS_{aH} open responder JFK_0

$m=g^x,\ n=g^y$
$k=g^{xy}$

STS STS_H JFK_1

protect identities

STS_P STS_{PH} JFK

symmetric hash

RFK

$$\xrightarrow{\quad m \quad}$$

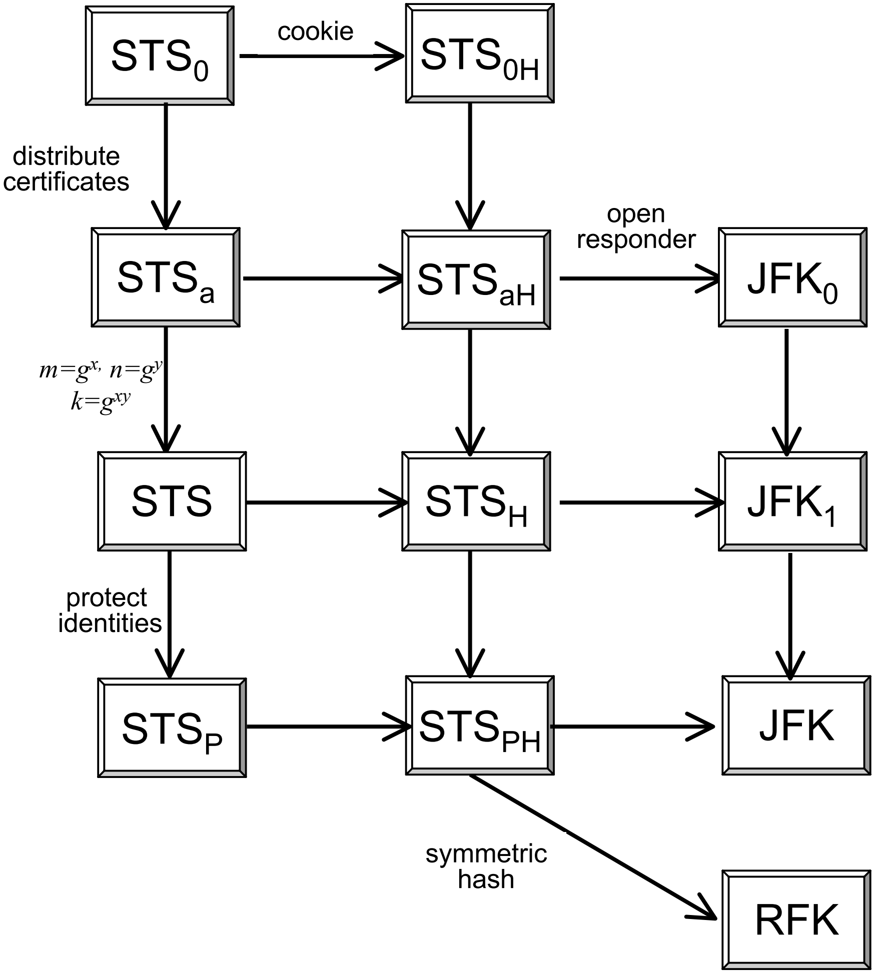
$$\xleftarrow{\quad n,\ H_{mn} \quad}$$

$$\xrightarrow{\quad m,\ n,\ H_{mn},\ C_A,\ E_k(S_A(m,n)) \quad}$$

$$\xleftarrow{\quad C_B,\ E_k(S_B(n,\ m)) \quad}$$

$m=g^x$
$n=g^y$
$k=g^{xy}$

STS family



$\xrightarrow{\quad m \quad}$

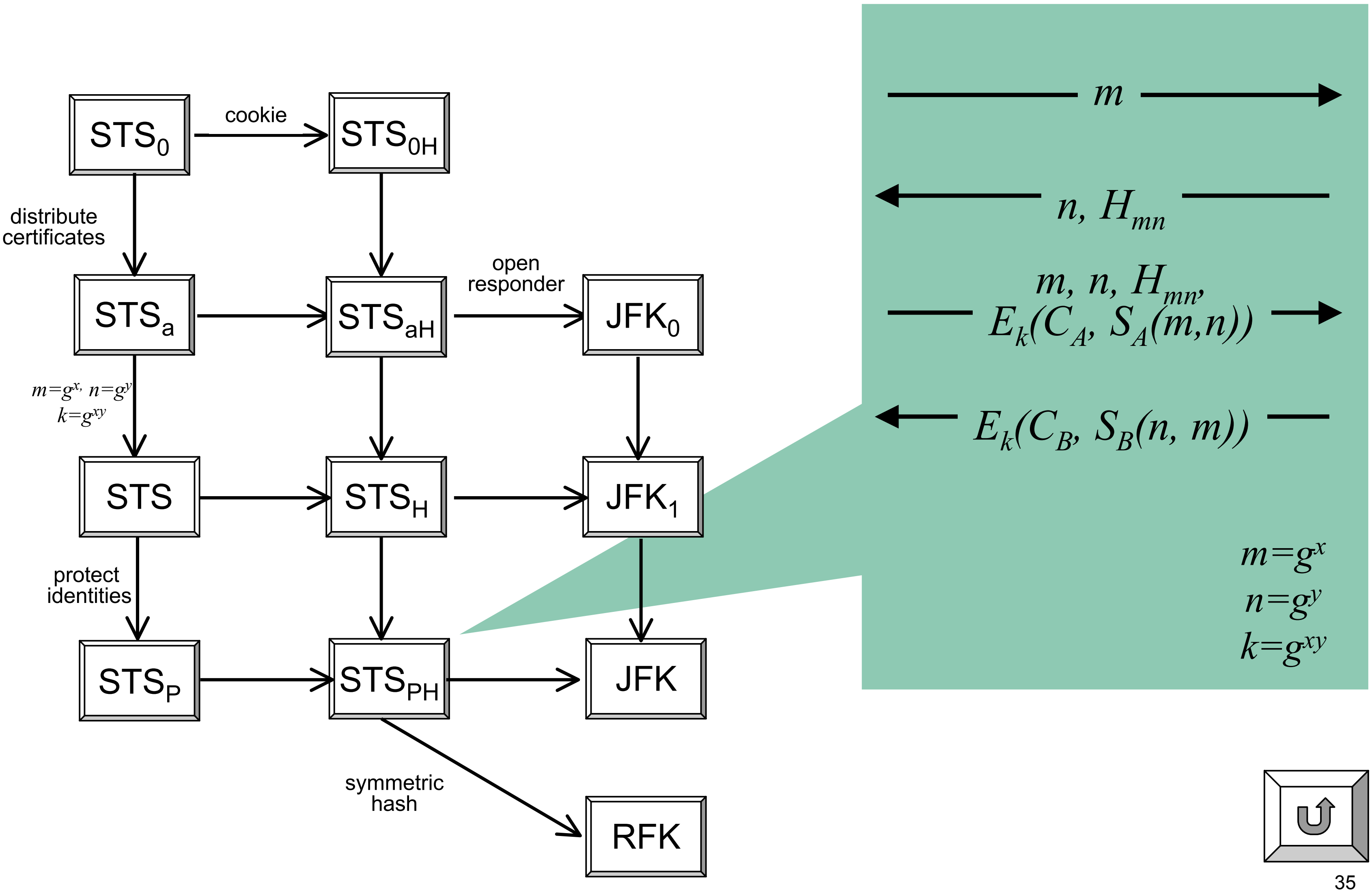
$\xleftarrow{\quad n, C_B, H_{mn} \quad}$

$\xrightarrow{\quad m, n, H_{mn}, C_A, E_k(S_A(m,n,C_B)) \quad}$

$\xleftarrow{\quad E_k(S_B(n, m)) \quad}$

$m=g^x$
$n=g^y$
$k=g^{xy}$

STS family



$\xrightarrow{\quad m \quad}$

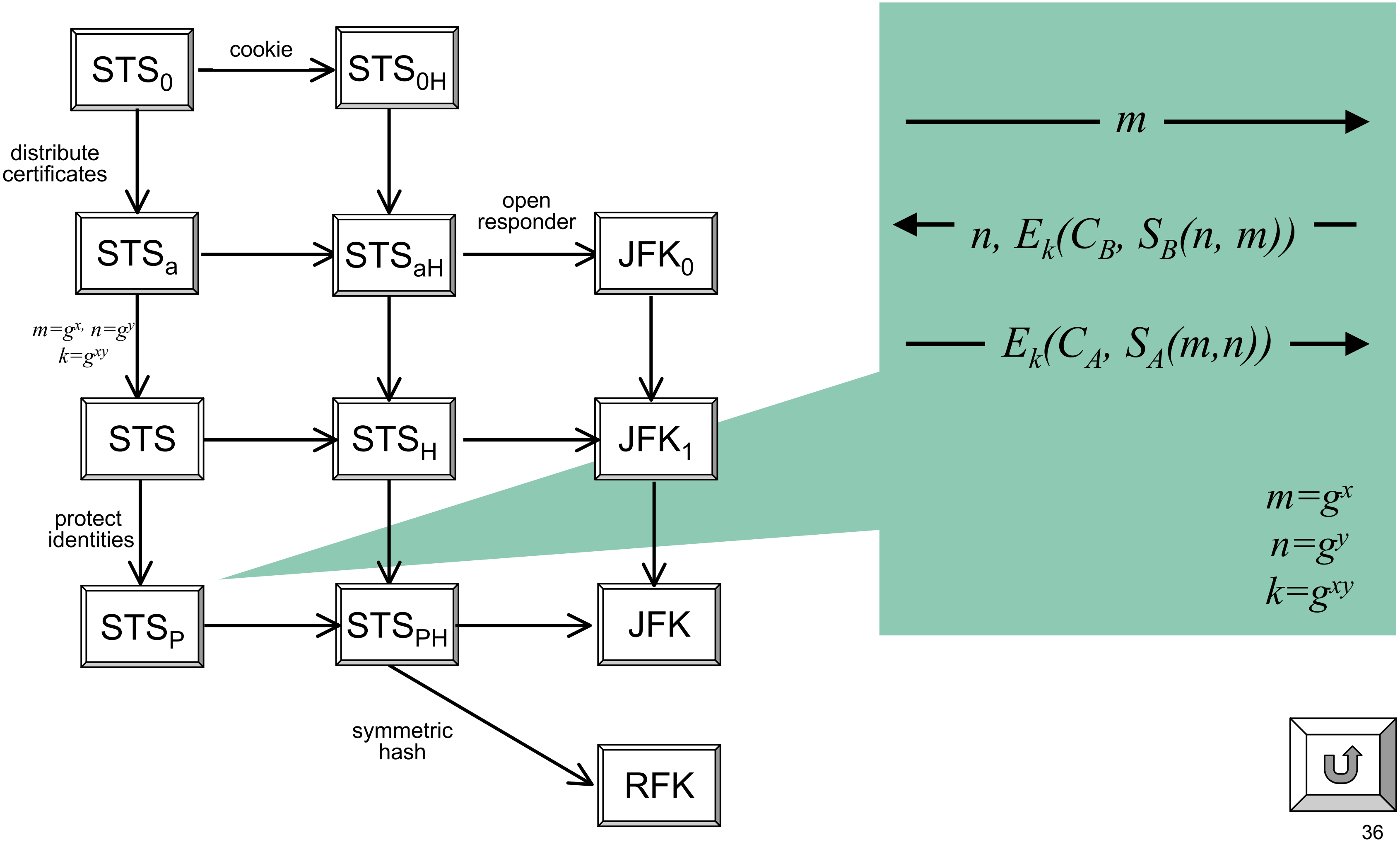
$\xleftarrow{\quad n, H_{mn} \quad}$

$\xrightarrow{\quad m, n, H_{mn}, E_k(C_A, S_A(m,n)) \quad}$

$\xleftarrow{\quad E_k(C_B, S_B(n, m)) \quad}$

$m=g^x$
$n=g^y$
$k=g^{xy}$

STS family



STS$_0$ —cookie→ STS$_{0H}$

STS$_0$ —distribute certificates→ STS$_a$

STS$_{0H}$ → STS$_{aH}$

STS$_a$ → STS$_{aH}$

STS$_{aH}$ —open responder→ JFK$_0$

STS$_a$ —$m{=}g^x$, $n{=}g^y$, $k{=}g^{xy}$→ STS

STS$_{aH}$ → STS$_H$

JFK$_0$ → JFK$_1$

STS → STS$_H$ → JFK$_1$

STS —protect identities→ STS$_P$

STS$_H$ → STS$_{PH}$

JFK$_1$ → JFK

STS$_P$ → STS$_{PH}$ → JFK

STS$_{PH}$ —symmetric hash→ RFK

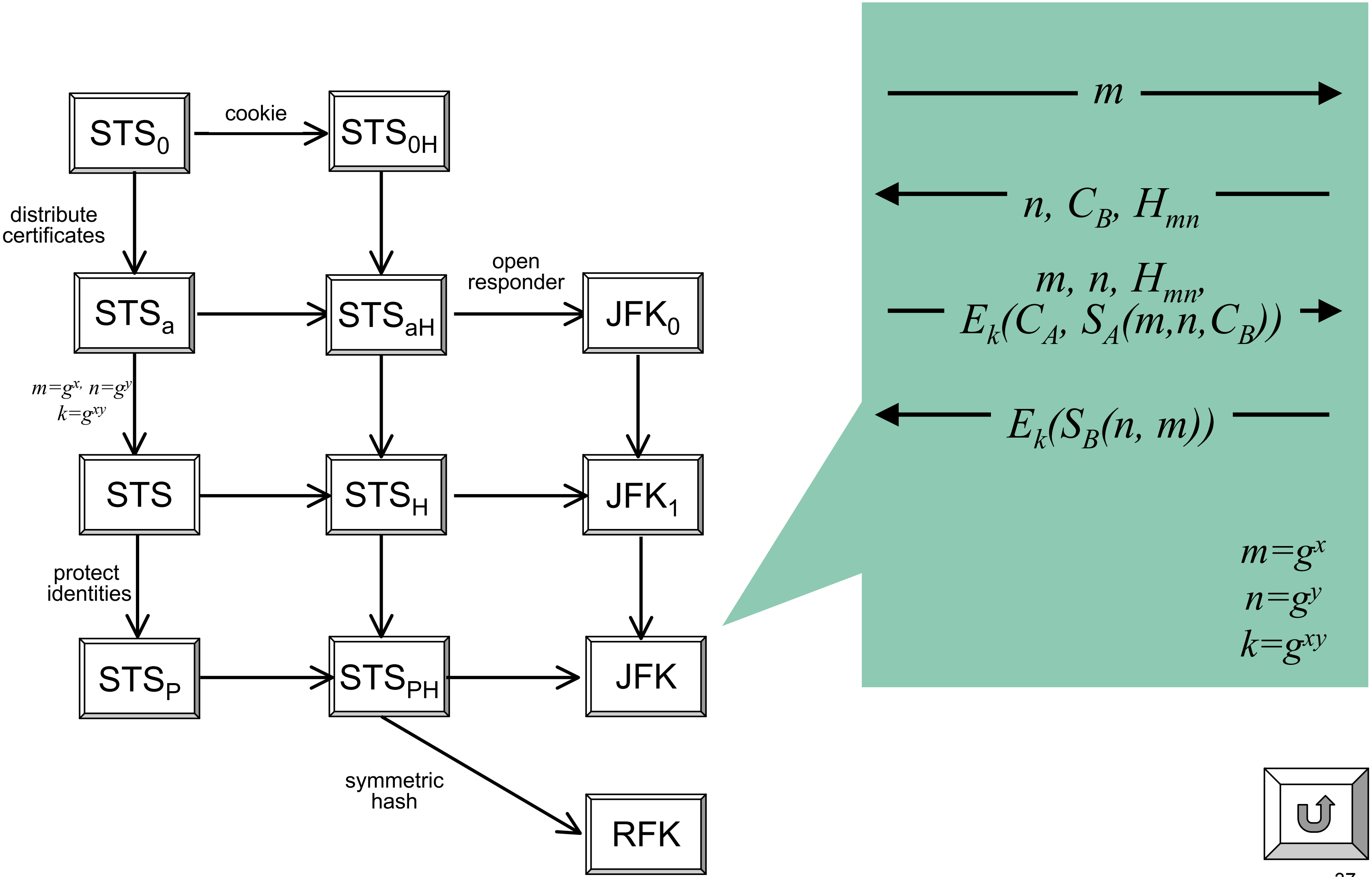
$$\xrightarrow{\quad m \quad}$$

$$\xleftarrow{\quad n,\ E_k(C_B,\ S_B(n,\ m)) \quad}$$

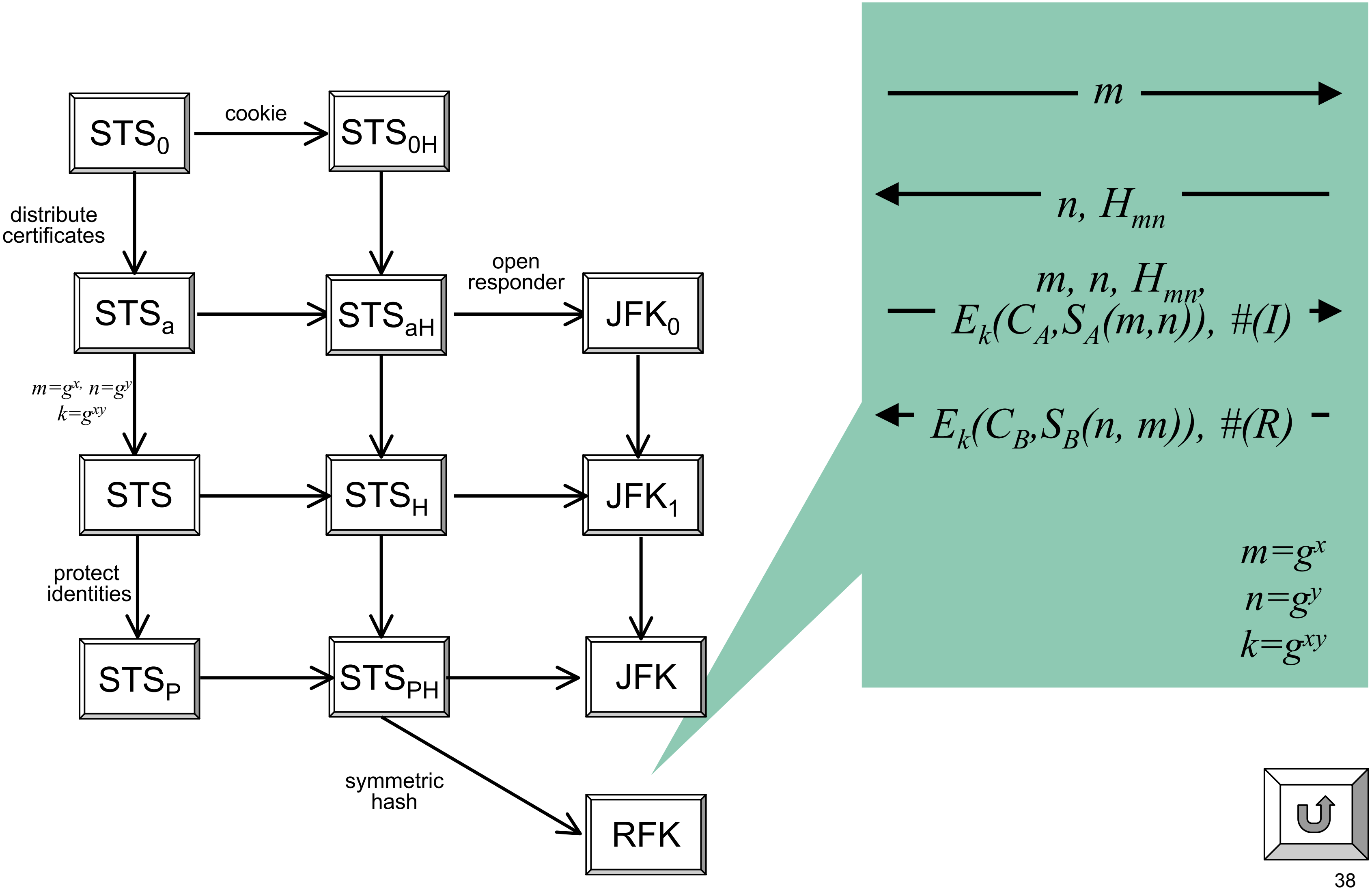
$$\xrightarrow{\quad E_k(C_A,\ S_A(m,n)) \quad}$$

$m{=}g^x$
$n{=}g^y$
$k{=}g^{xy}$

STS family


STS_0
cookie
STS_{0H}
distribute certificates
STS_a
STS_{aH}
open responder
JFK_0
$m=g^x, n=g^y$
$k=g^{xy}$
STS
STS_H
JFK_1
protect identities
STS_P
STS_{PH}
JFK
symmetric hash
RFK
m
n, C_B, H_{mn}
$m, n, H_{mn}, E_k(C_A, S_A(m,n,C_B))$
$E_k(S_B(n, m))$
$m=g^x$
$n=g^y$
$k=g^{xy}$

STS family



$$\xrightarrow{\quad m \quad}$$

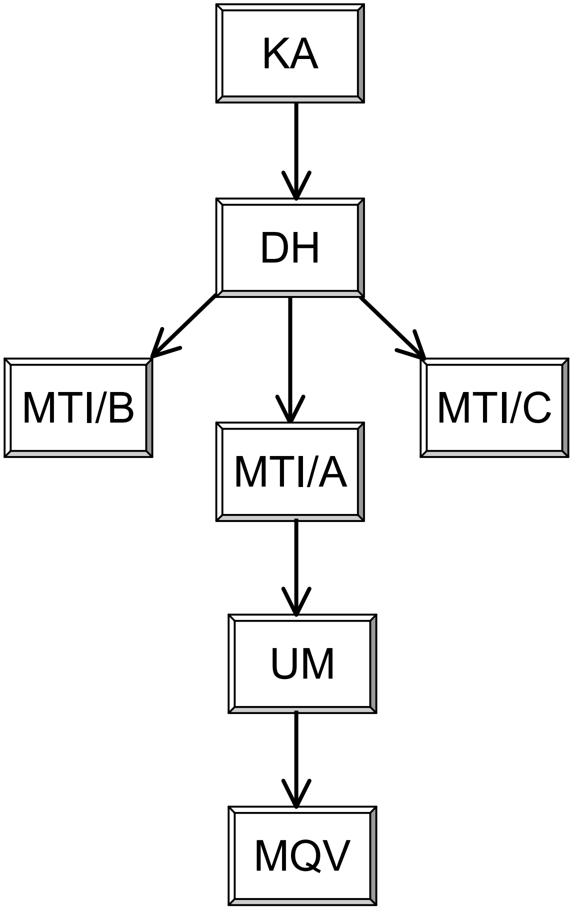
$$\xleftarrow{\quad n,\ H_{mn} \quad}$$

$$\xrightarrow{\quad m,\ n,\ H_{mn},\ E_k(C_A, S_A(m,n)),\ \#(I) \quad}$$

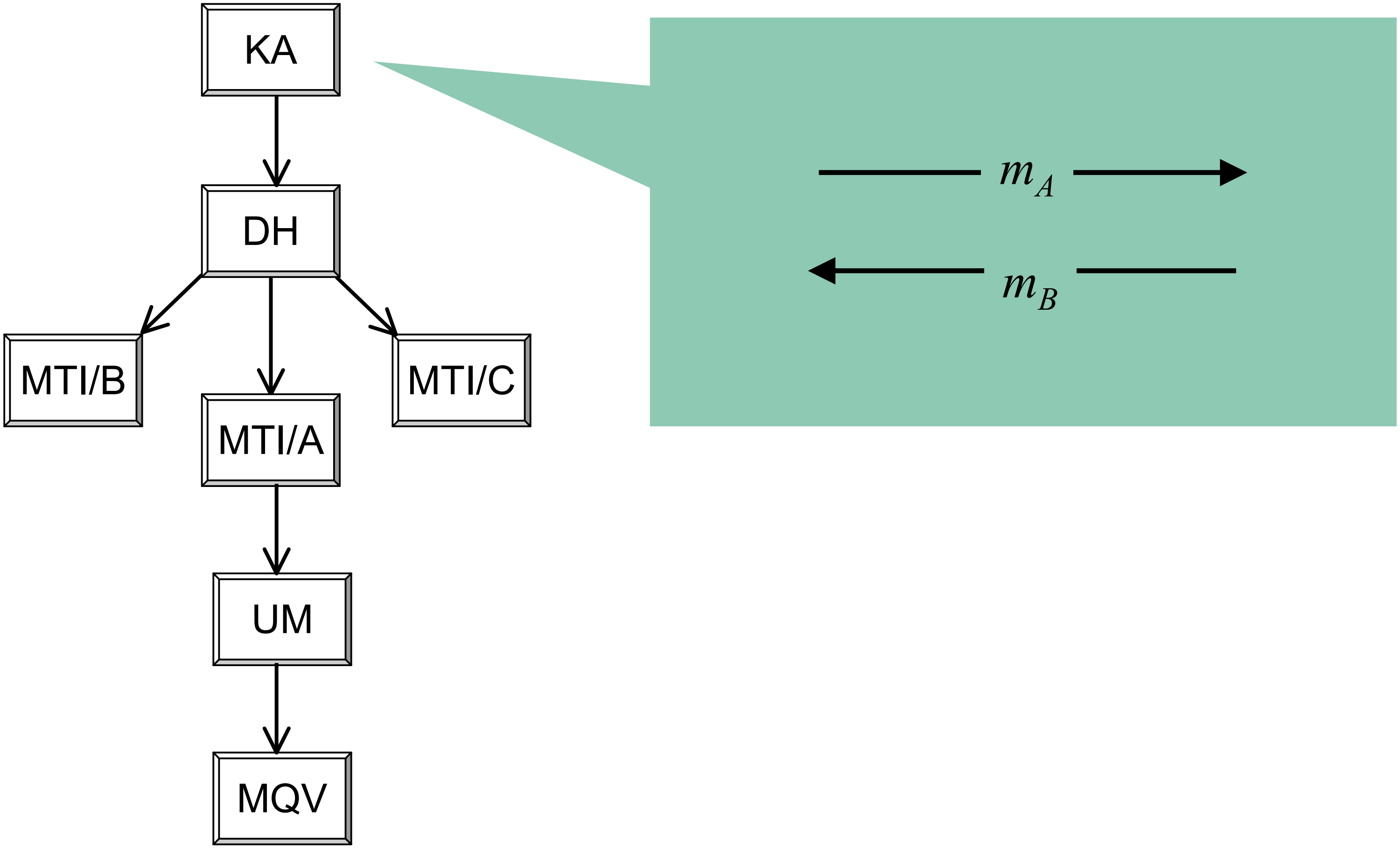
$$\xleftarrow{\quad E_k(C_B, S_B(n,\ m)),\ \#(R) \quad}$$

$m{=}g^x$
$n{=}g^y$
$k{=}g^{xy}$

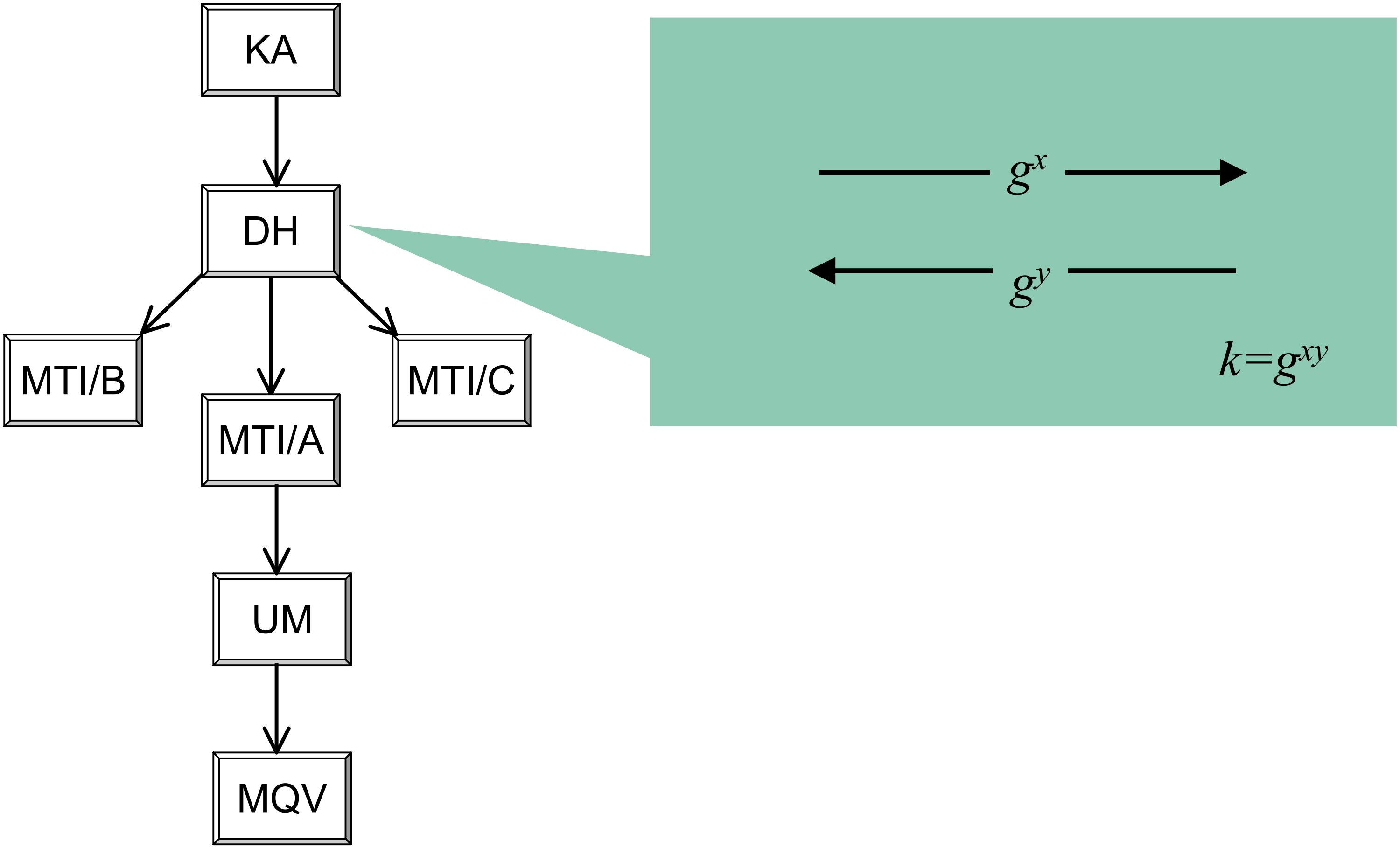
MQV family



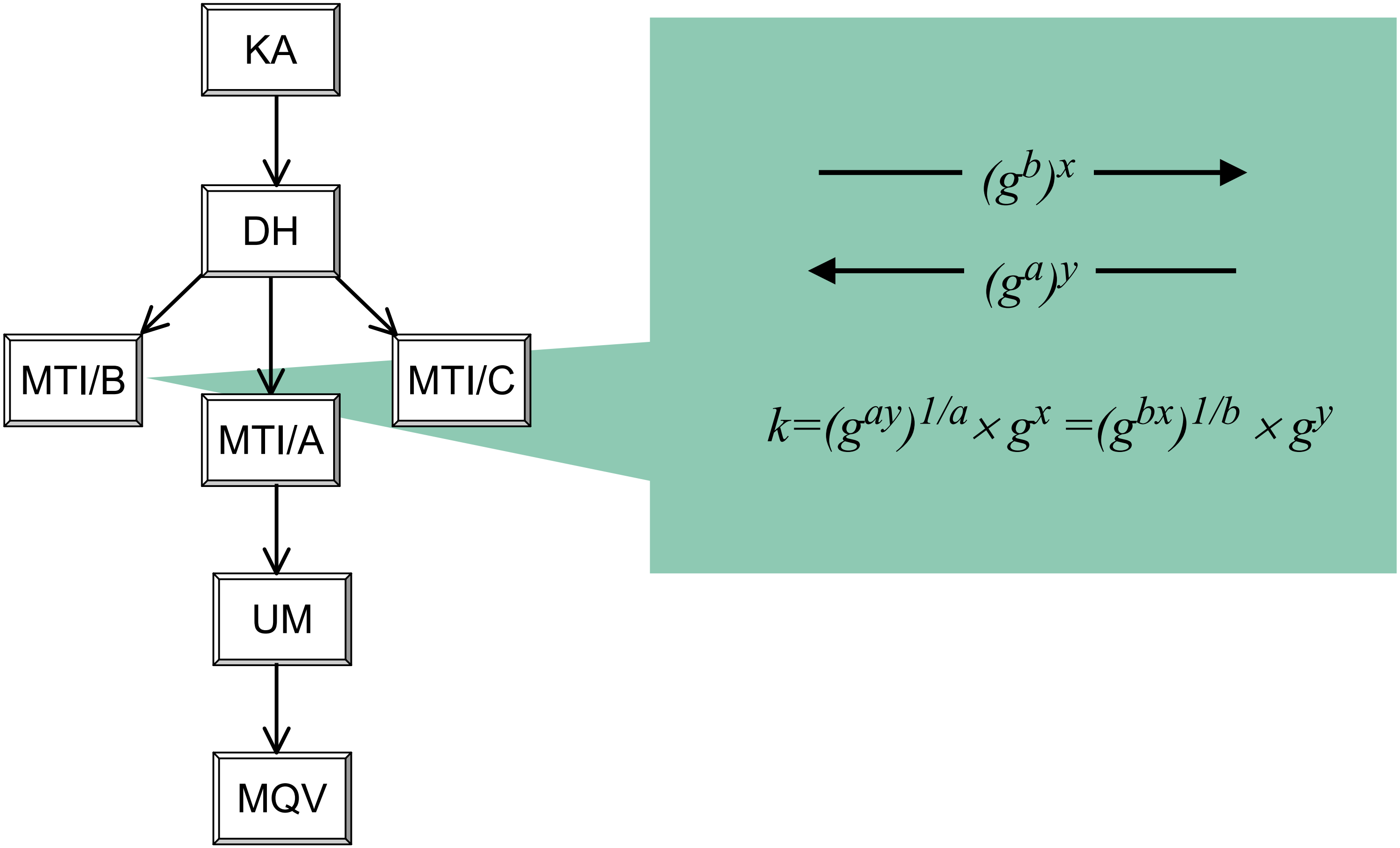
MQV family



MQV family



MQV family

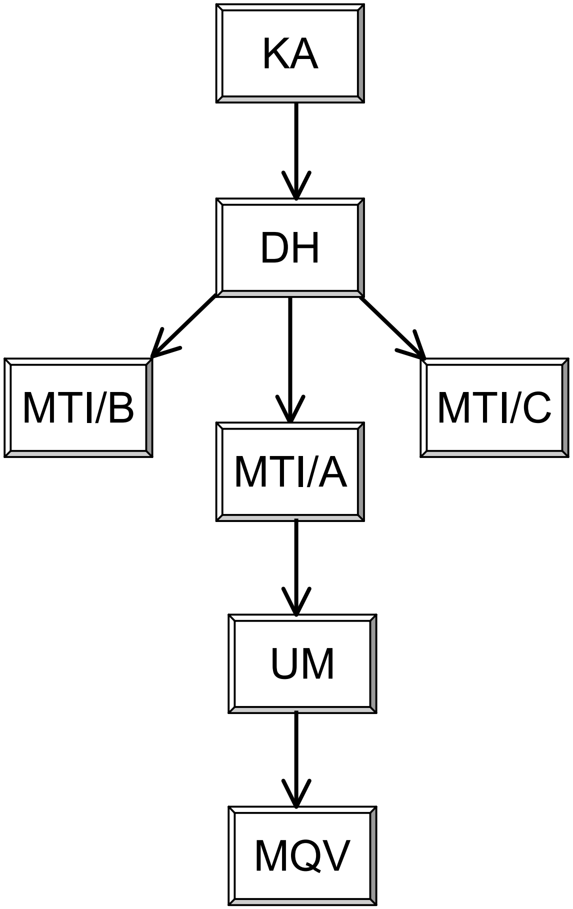


$$\xrightarrow{(g^b)^x}$$

$$\xleftarrow{(g^a)^y}$$

$$k=(g^{ay})^{1/a}\times g^x=(g^{bx})^{1/b}\times g^y$$

MQV family


KA

DH

MTI/B

MTI/A

MTI/C

UM

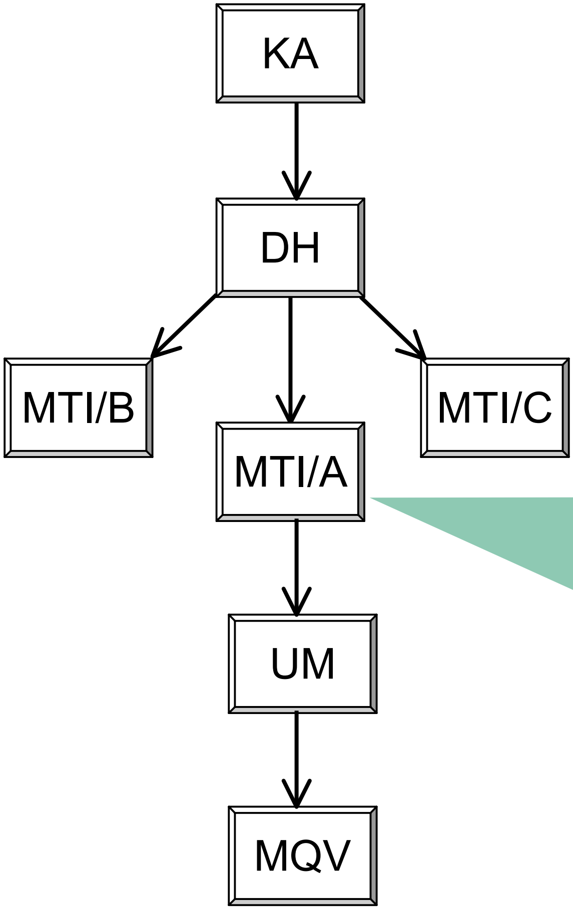
MQV

$$\xrightarrow{\quad (g^b)^x \quad}$$

$$\xleftarrow{\quad (g^a)^y \quad}$$

$$k=(g^{ay})^{x/a}=(g^{bx})^{y/b}$$

MQV family



KA

DH

MTI/B

MTI/A

MTI/C

UM

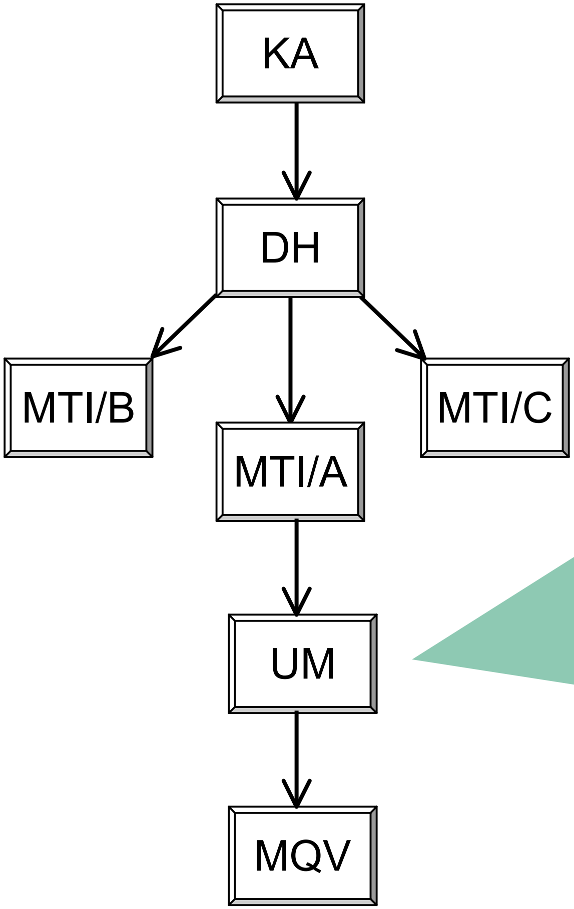
MQV

$$\xrightarrow{g^x,\ G_A} \qquad G_A=\{A,g^a\}_{TA}$$

$$\xleftarrow{g^y,\ G_B} \qquad G_B=\{B,g^b\}_{TA}$$

$$\begin{aligned} k &= \{(g^y)^a \times (g^b)^x\} \\ &= \{(g^x)^b \times (g^a)^y\} \end{aligned}$$

MQV family



$\longrightarrow g^x, G_A \longrightarrow$ $\quad G_A=\{A,g^a\}_{TA}$

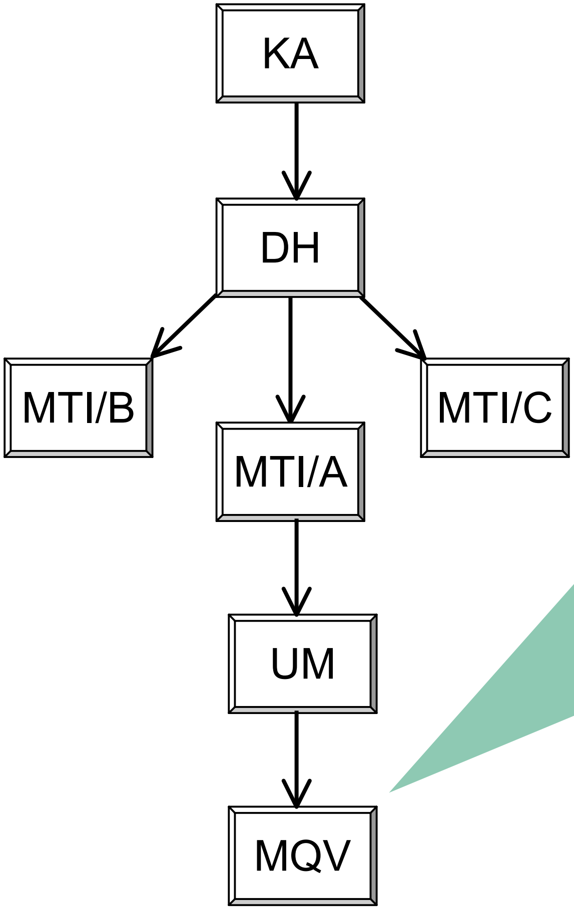
$\longleftarrow g^y, G_B \longleftarrow$ $\quad G_B=\{B,g^b\}_{TA}$

$$k = \{(g^y)^a \,||\, (g^b)^x\} = \{(g^x)^b \,||\, (g^a)^y\}$$

or

$$k = \{(g^y)^x \,||\, (g^b)^a\} = \{(g^x)^y \,||\, (g^a)^b\}$$

MQV family



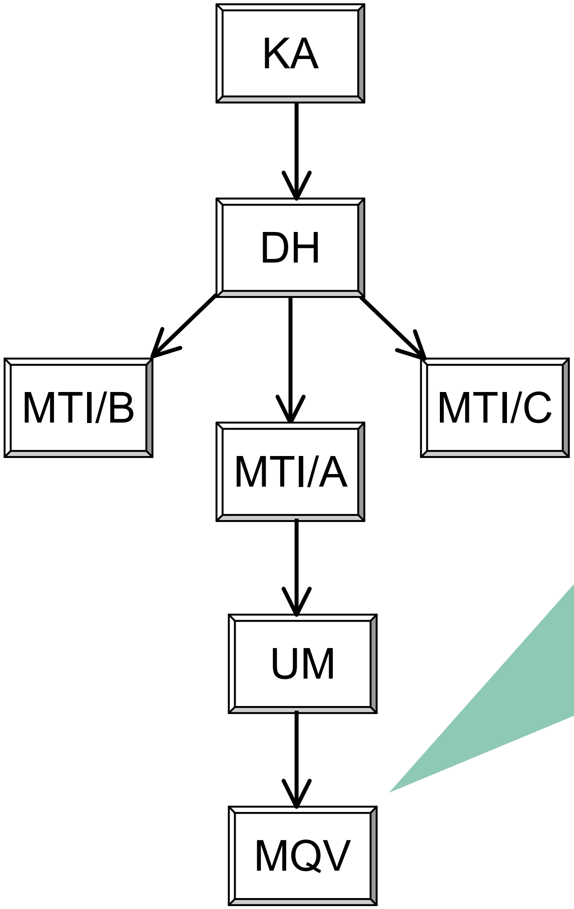
$$— \; g^x,\ G_A \longrightarrow \qquad G_A=\{A,g^a\}_{TA}$$

$$\longleftarrow \; g^y,\ G_B \; — \qquad G_B=\{B,g^b\}_{TA}$$

$$k = g^{f(a,x) \times f(b,y)} \qquad \text{where}$$

$$f(a,x) = ag^x + x$$

MQV family



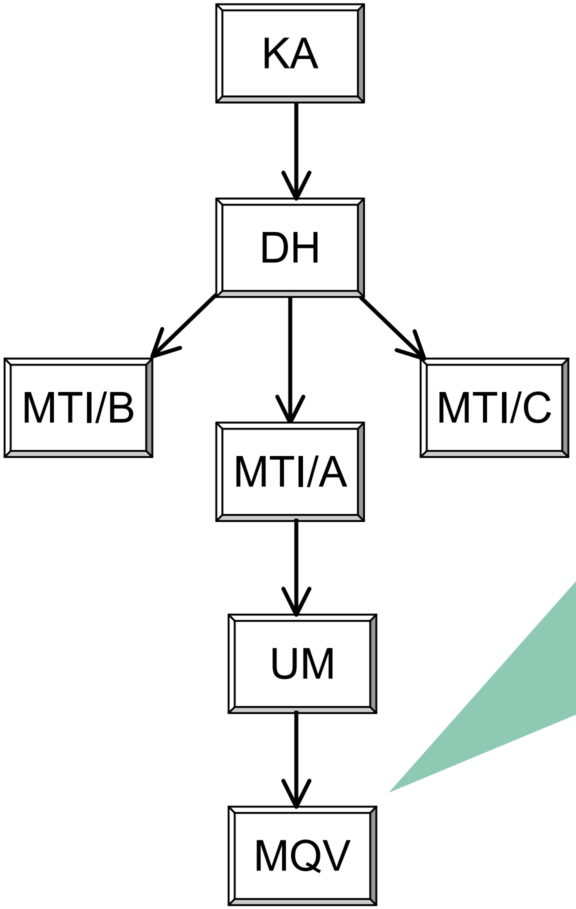
$$\text{—}\ g^x,\ G_A \longrightarrow \qquad G_A=\{A,g^a\}_{TA}$$

$$\longleftarrow g^y\ ,\ G_B\ \text{—} \qquad G_B=\{B,g^b\}_{TA}$$

$$k = g^{f(a,x)\ \times\ f(b,y)} \qquad \text{where}$$

$$f(a,x) = ag^x + x$$

MQV family



KA

DH

MTI/B

MTI/A

MTI/C

UM

MQV

$\xrightarrow{\quad g^x,\ G_A \quad}$ $\qquad G_A=\{A,g^a\}_{TA}$

$\xleftarrow{\quad g^y,\ G_B \quad}$ $\qquad G_B=\{B,g^b\}_{TA}$

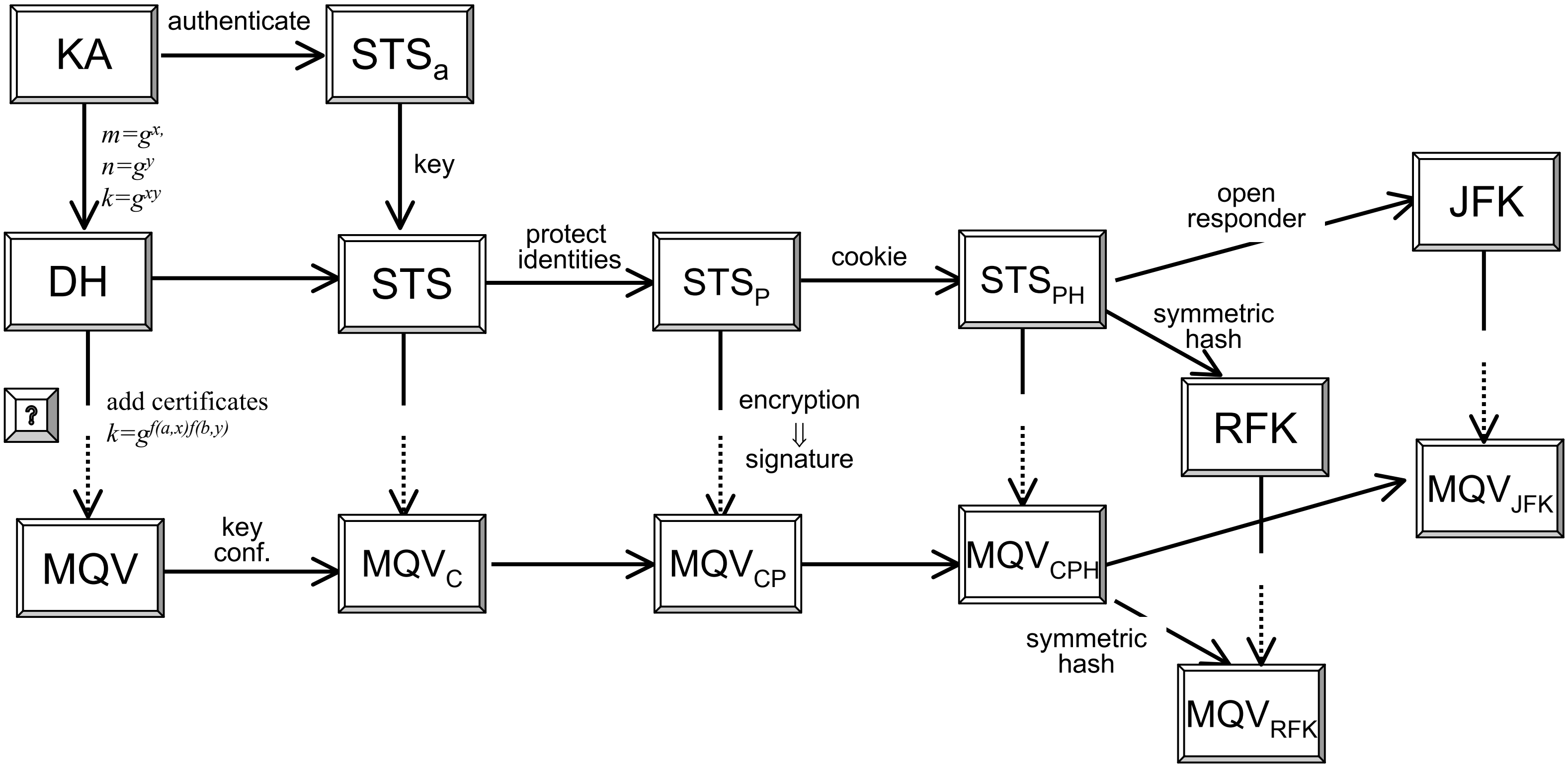
$k = g^{f(a,x)\times f(b,y)}$ where

$g^{f(a,x)} = F(g^a, g^x)$ is 1-way in g^x.

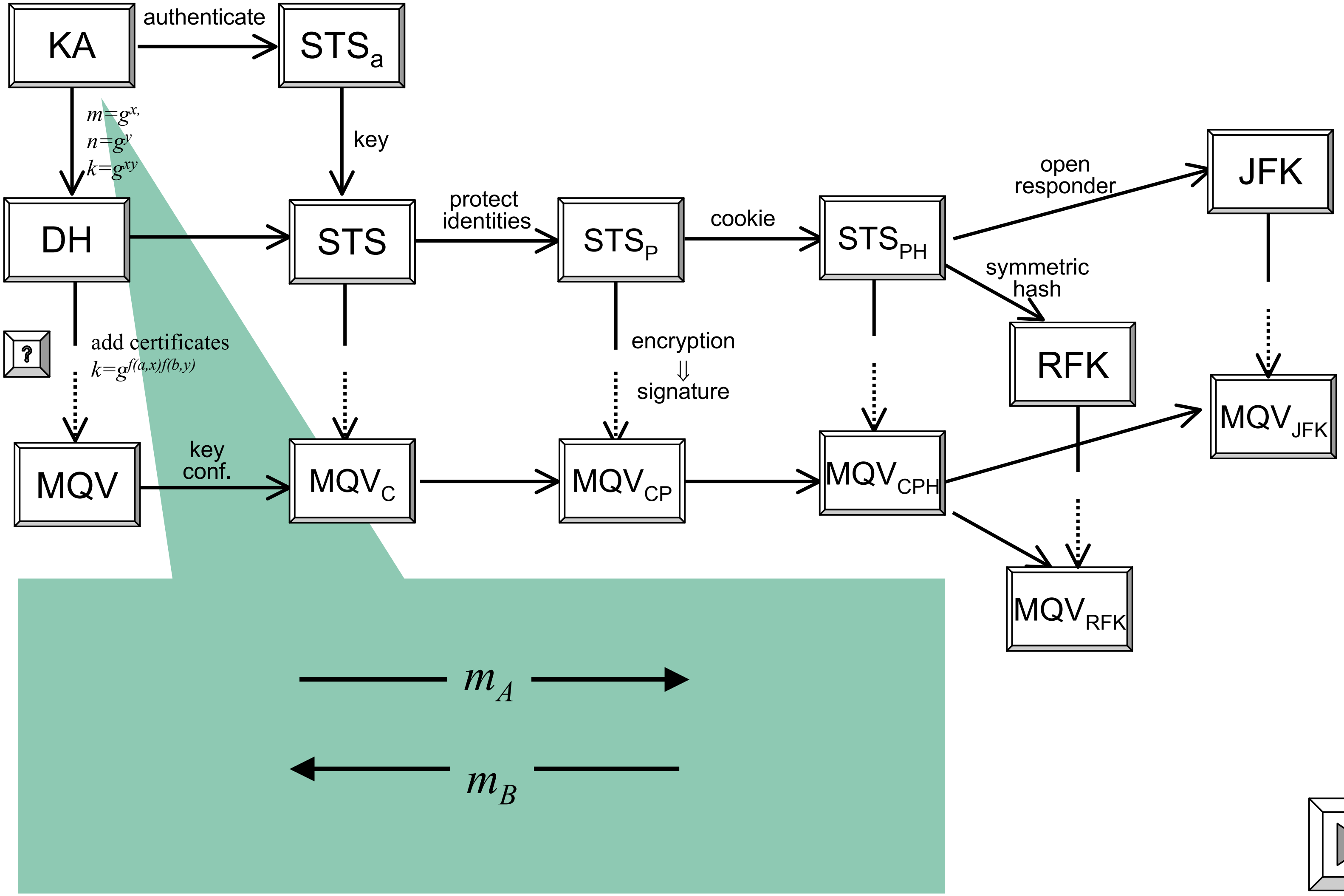
E.g., given a one-way function $H(n)$, such that $H(g^x) = g^{h(x)}$, take

$F(m,n)= m\times H(n)$ and $f(a,x) = a+h(x)$

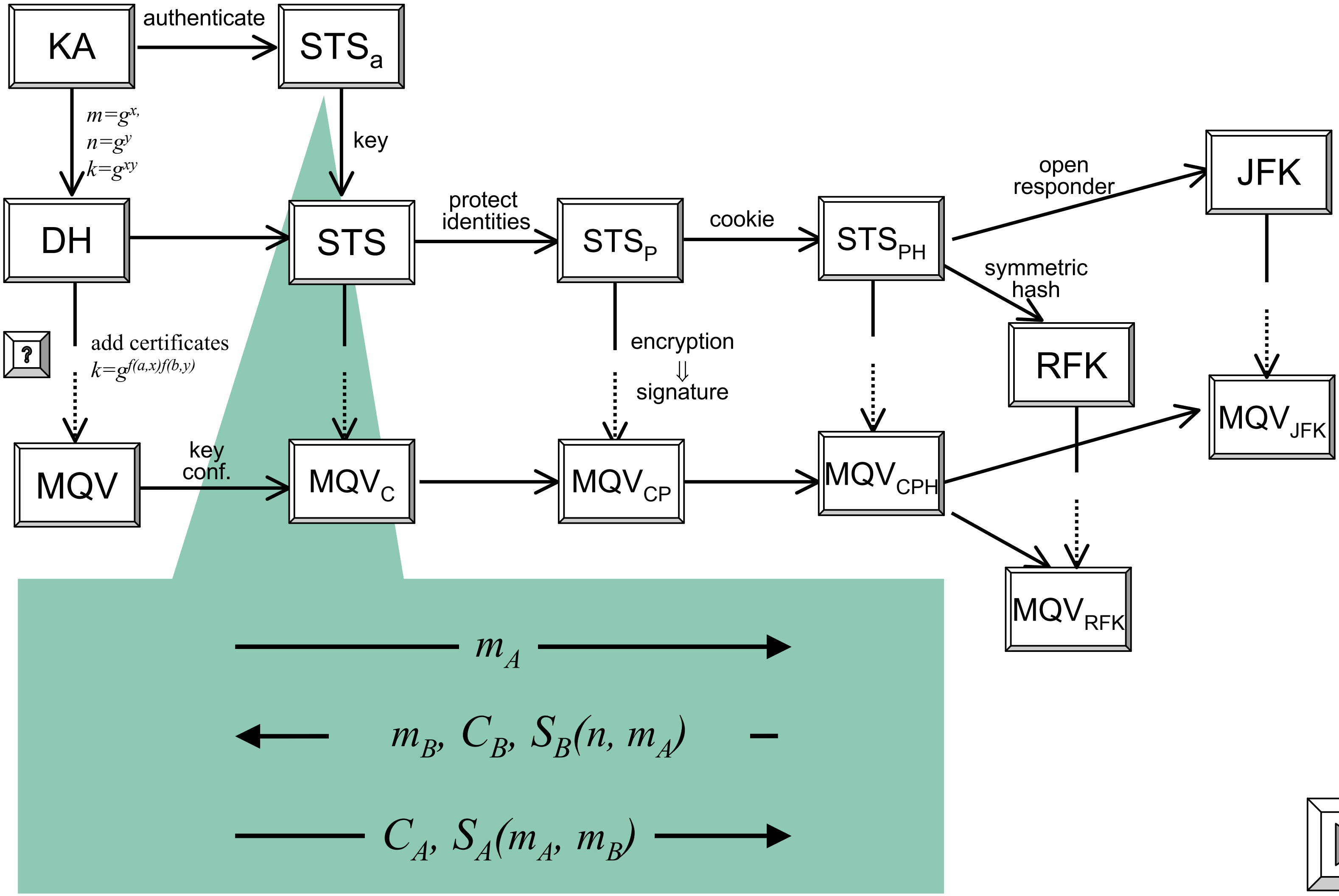
MQV refinements



MQV refinements



MQV refinements

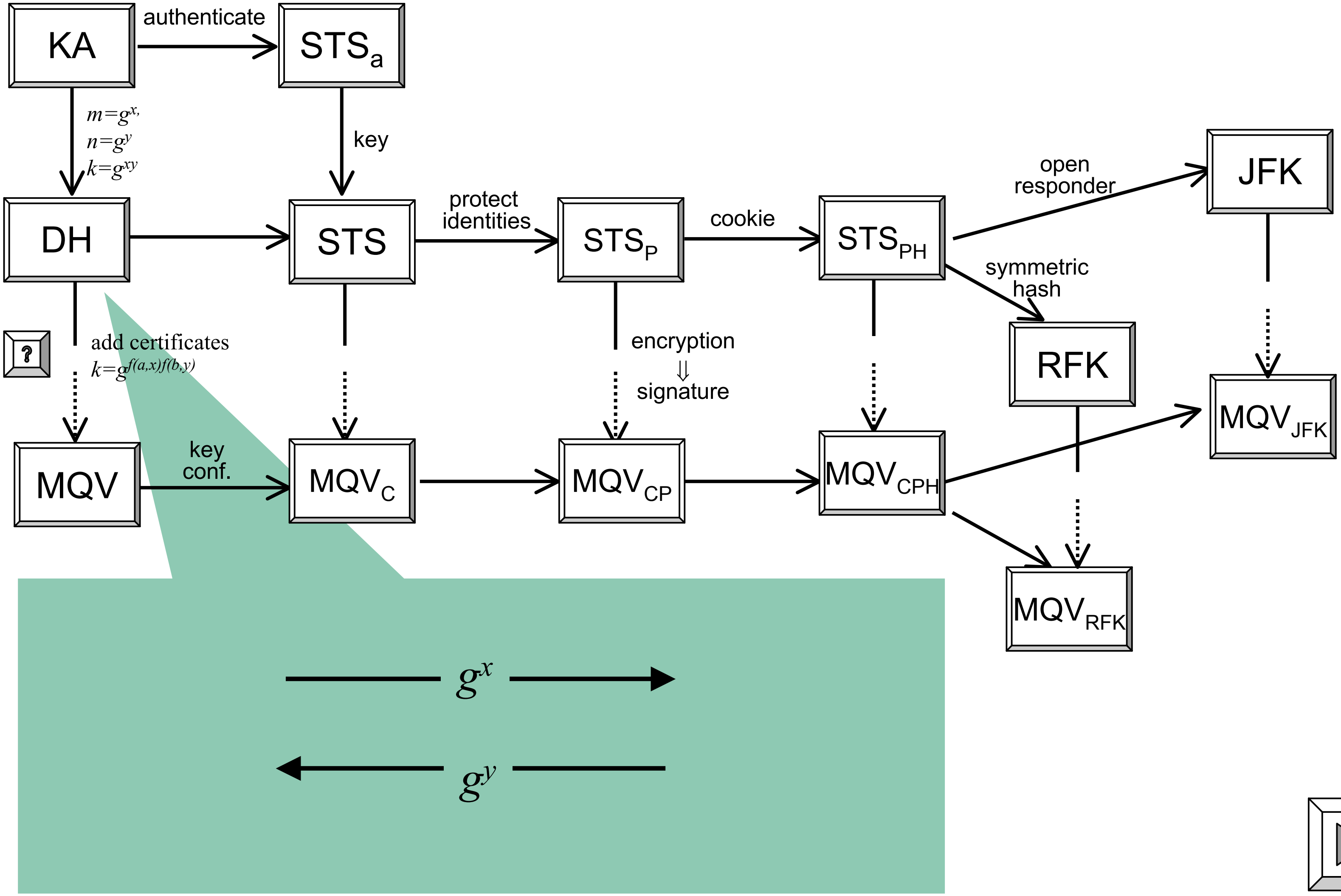


$$\xrightarrow{\quad m_A \quad}$$

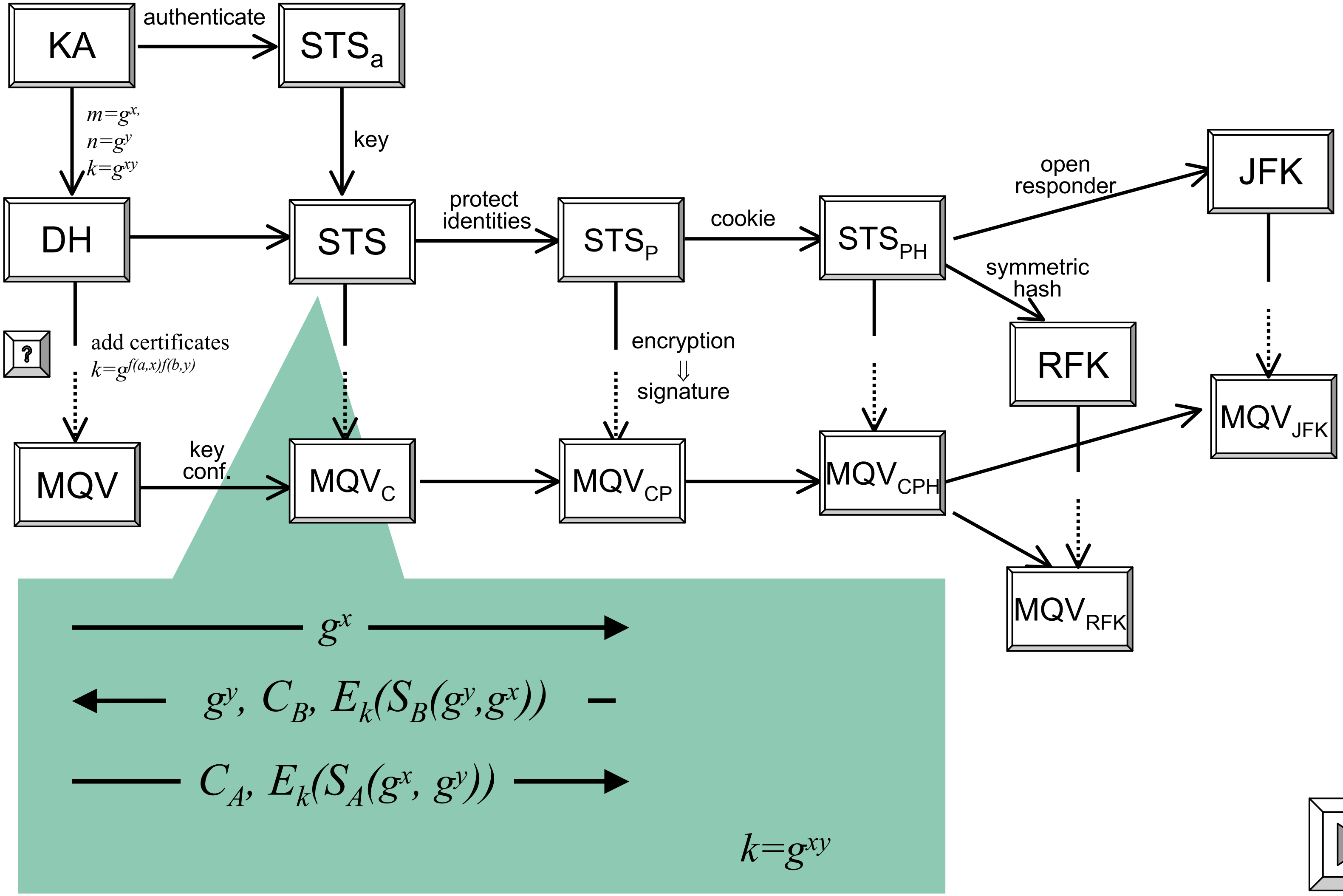
$$\xleftarrow{\quad m_B,\ C_B,\ S_B(n,\ m_A) \quad}$$

$$\xrightarrow{\quad C_A,\ S_A(m_A,\ m_B) \quad}$$

MQV refinements



MQV refinements



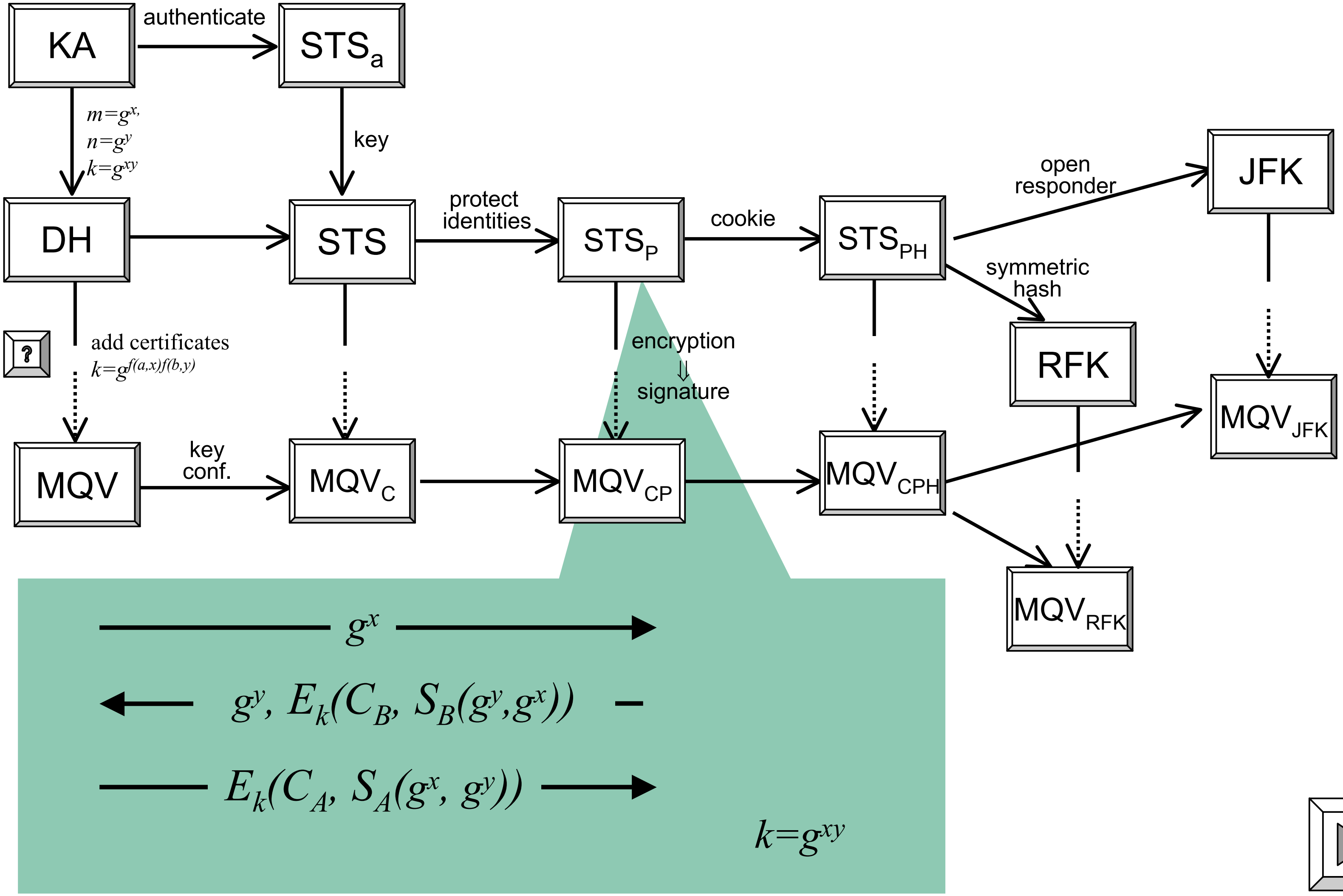
$$\xrightarrow{\quad g^x \quad}$$

$$\xleftarrow{\quad g^y,\ C_B,\ E_k(S_B(g^y,g^x)) \quad}$$

$$\xrightarrow{\quad C_A,\ E_k(S_A(g^x,\ g^y)) \quad}$$

$k=g^{xy}$

MQV refinements



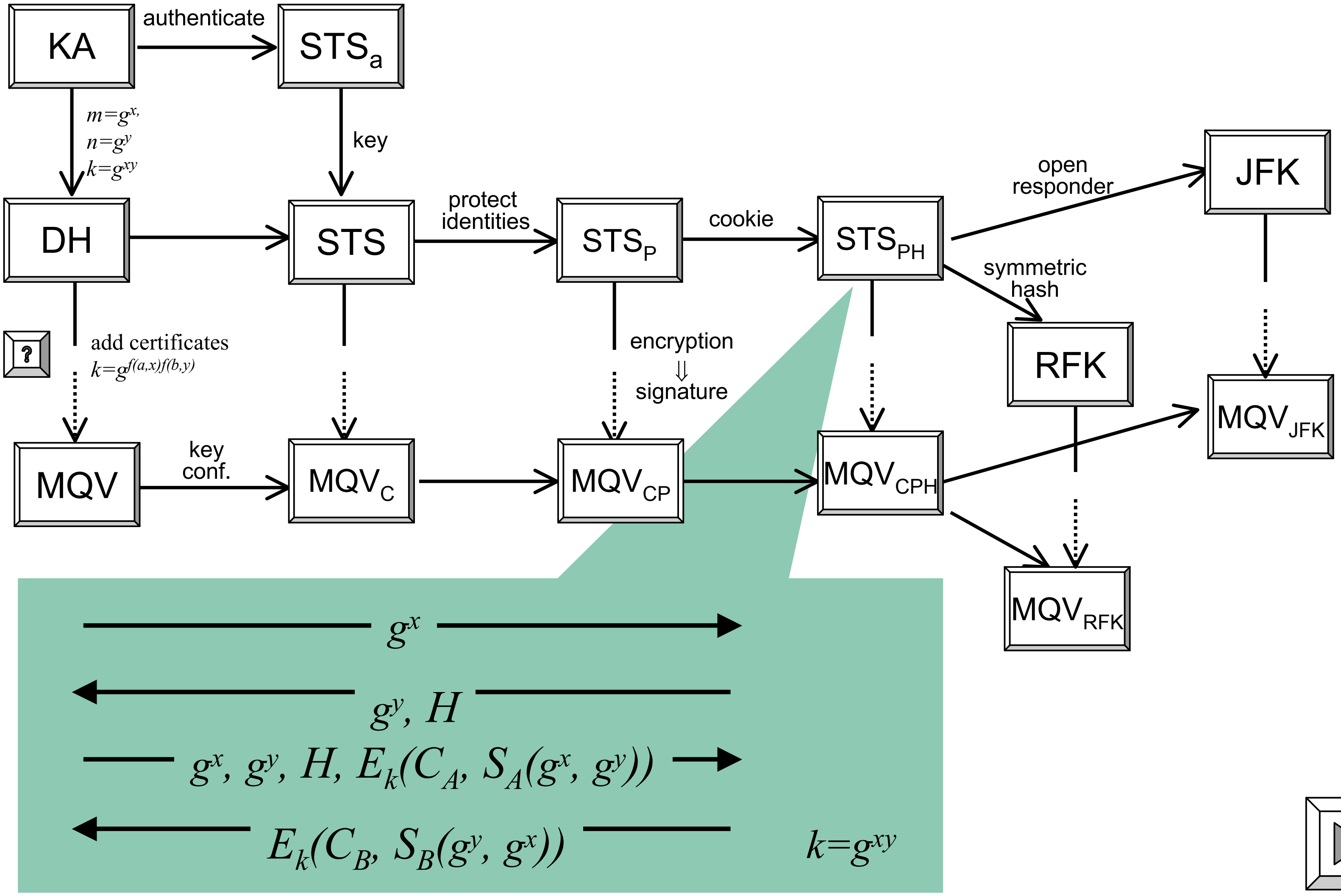
$$g^x \longrightarrow$$

$$\longleftarrow g^y, E_k(C_B, S_B(g^y,g^x))$$

$$E_k(C_A, S_A(g^x, g^y)) \longrightarrow$$

$k=g^{xy}$

MQV refinements



g^x →

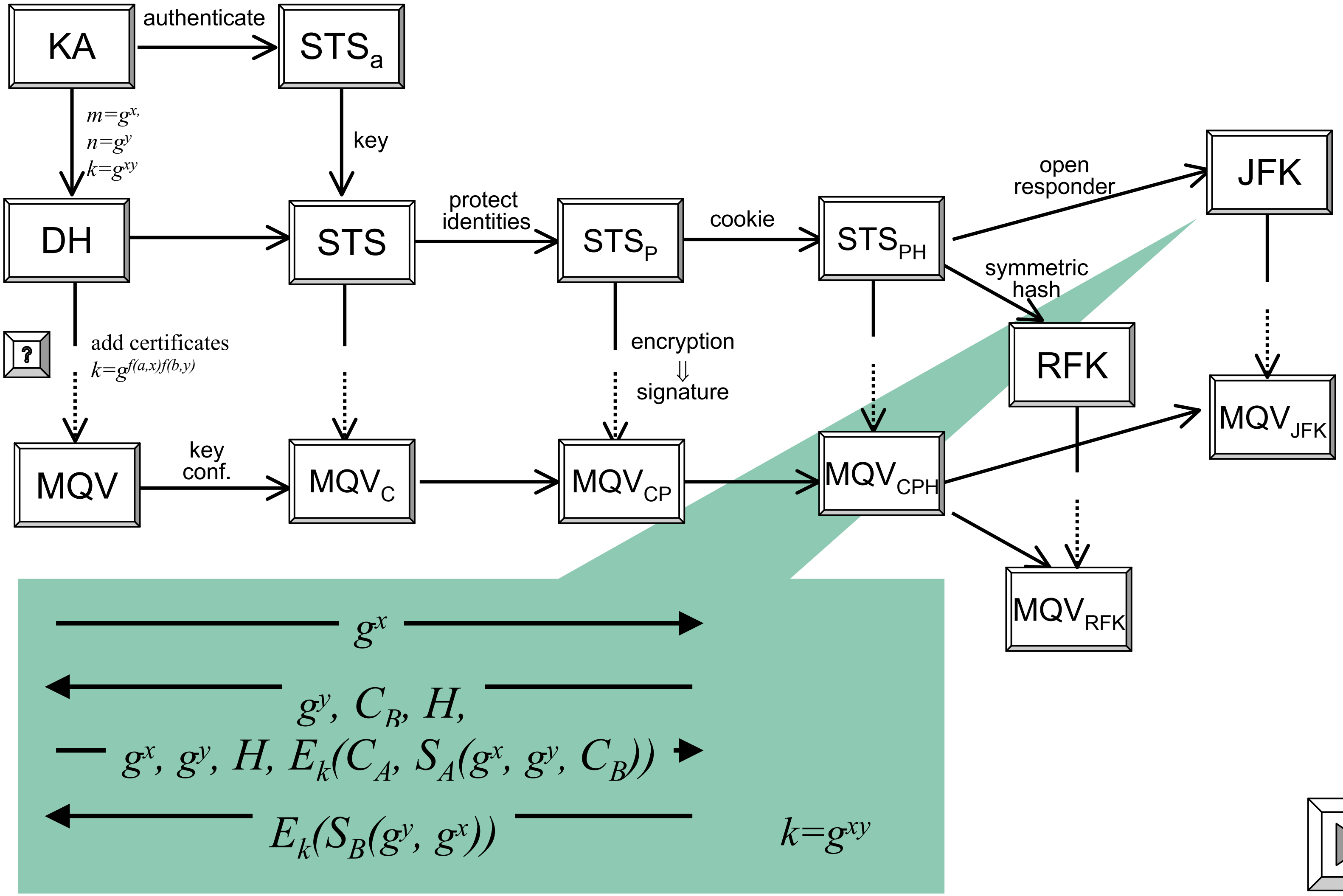
← g^y, H

$g^x, g^y, H, E_k(C_A, S_A(g^x, g^y))$ →

← $E_k(C_B, S_B(g^y, g^x))$

$k=g^{xy}$

MQV refinements



$$g^x \rightarrow$$

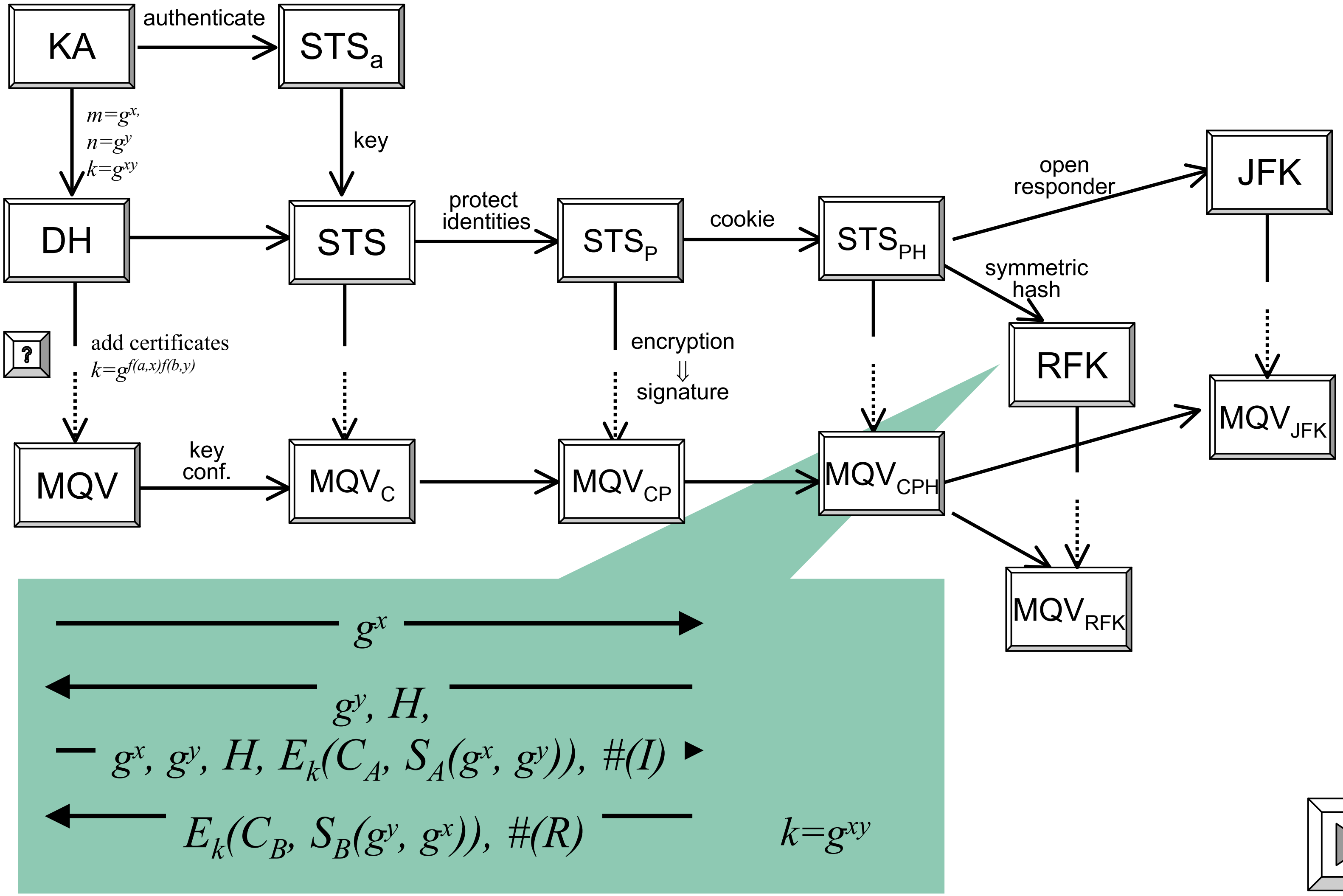
$$\leftarrow g^y,\ C_B,\ H,$$

$$g^x,\ g^y,\ H,\ E_k(C_A,\ S_A(g^x,\ g^y,\ C_B)) \rightarrow$$

$$\leftarrow E_k(S_B(g^y,\ g^x))$$

$$k=g^{xy}$$

MQV refinements



g^x →

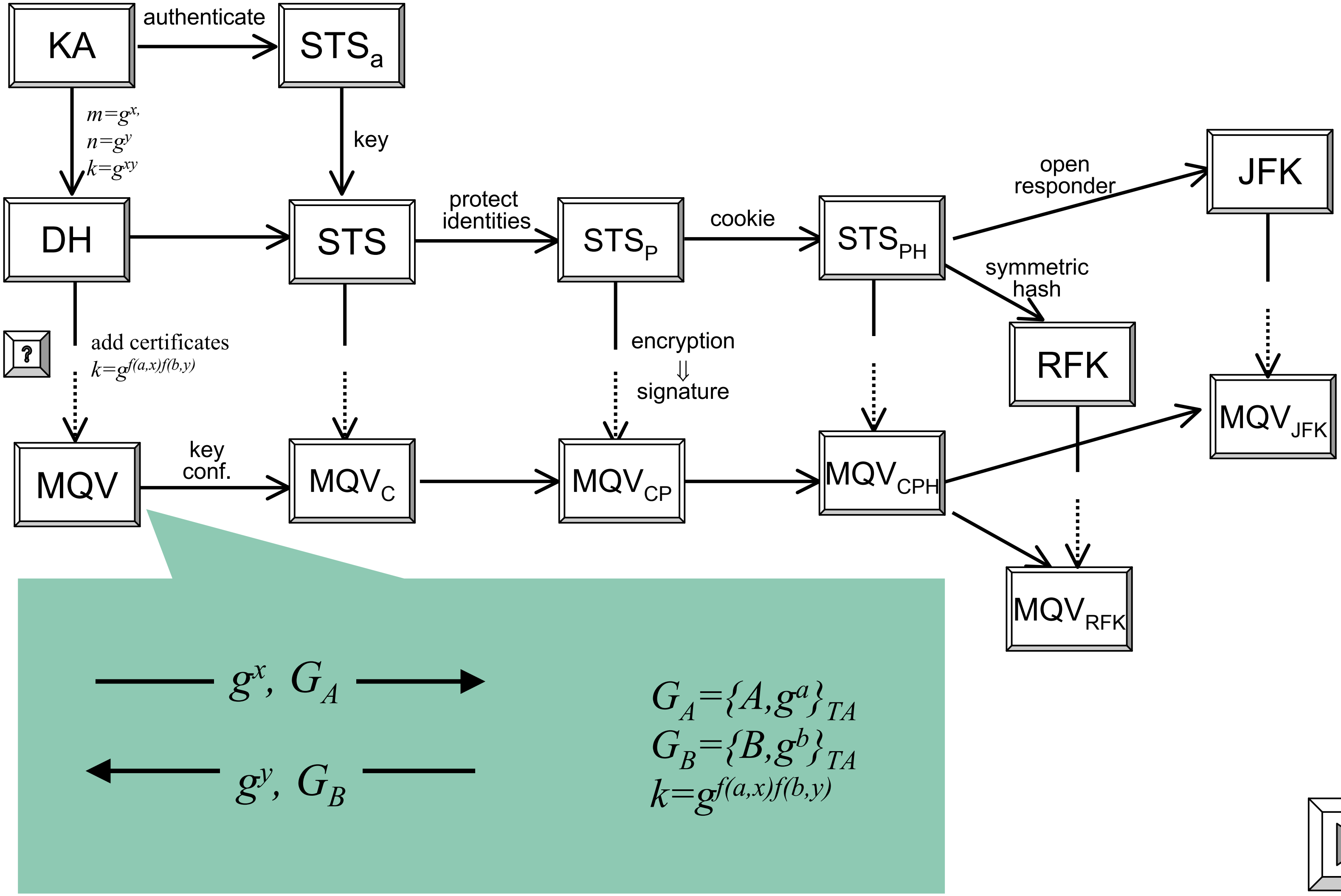
← $g^y, H,$

$g^x, g^y, H, E_k(C_A, S_A(g^x, g^y)), \#(I)$ →

← $E_k(C_B, S_B(g^y, g^x)), \#(R)$

$k=g^{xy}$

MQV refinements

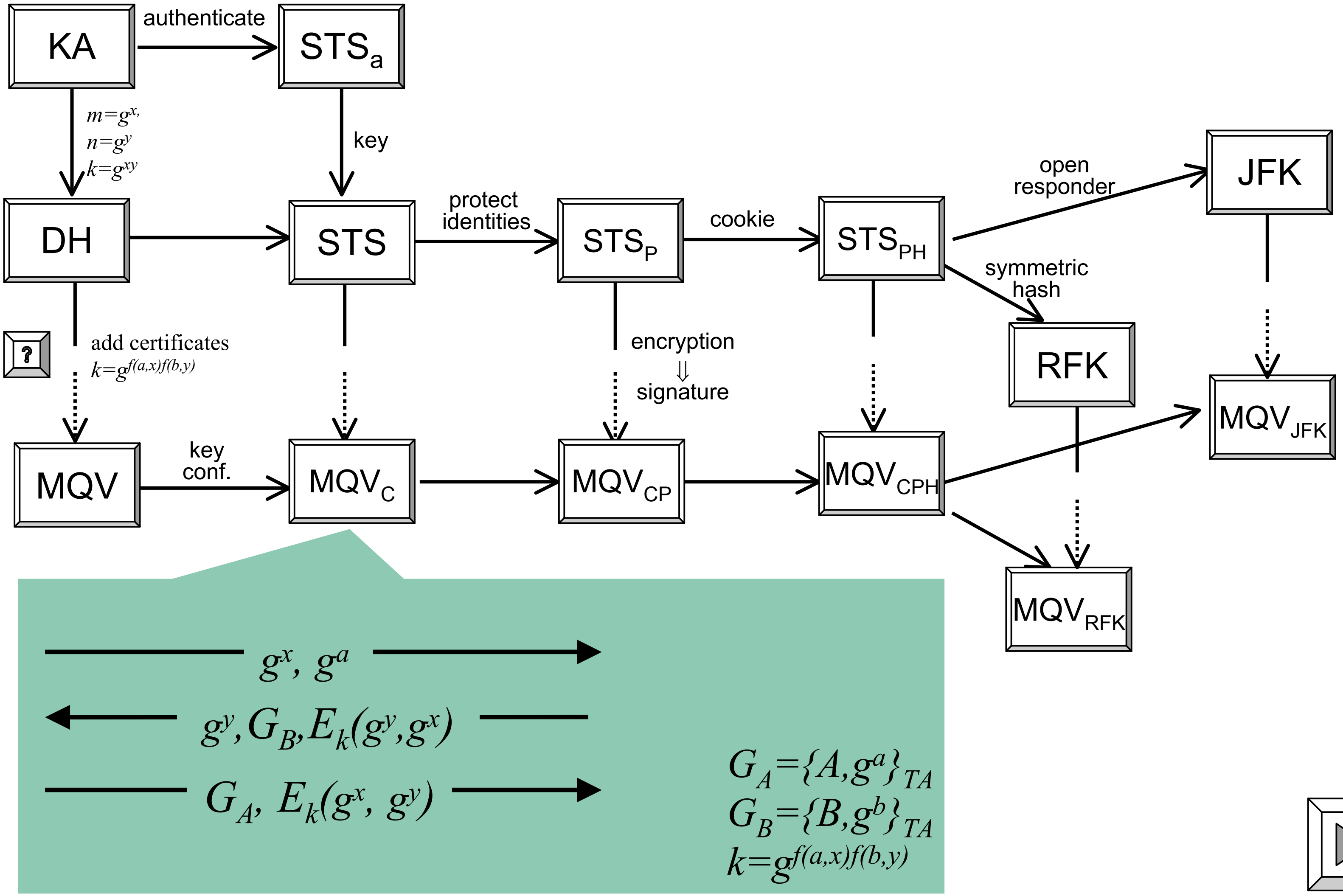


$$\xrightarrow{\quad g^x,\ G_A \quad}$$

$$\xleftarrow{\quad g^y,\ G_B \quad}$$

$$G_A=\{A,g^a\}_{TA}$$
$$G_B=\{B,g^b\}_{TA}$$
$$k=g^{f(a,x)f(b,y)}$$

MQV refinements



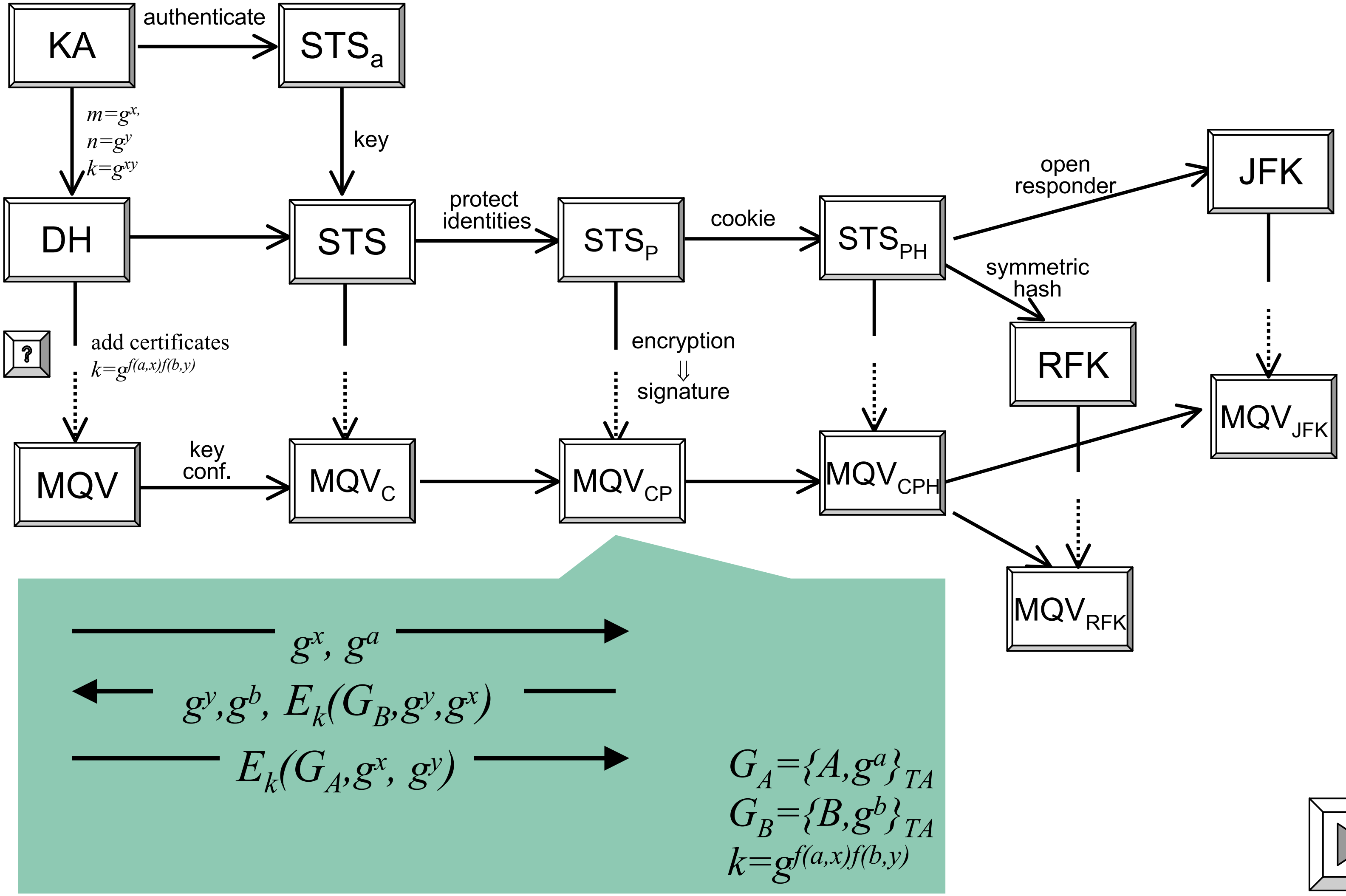
$g^x, g^a \longrightarrow$

$\longleftarrow g^y, G_B, E_k(g^y, g^x)$

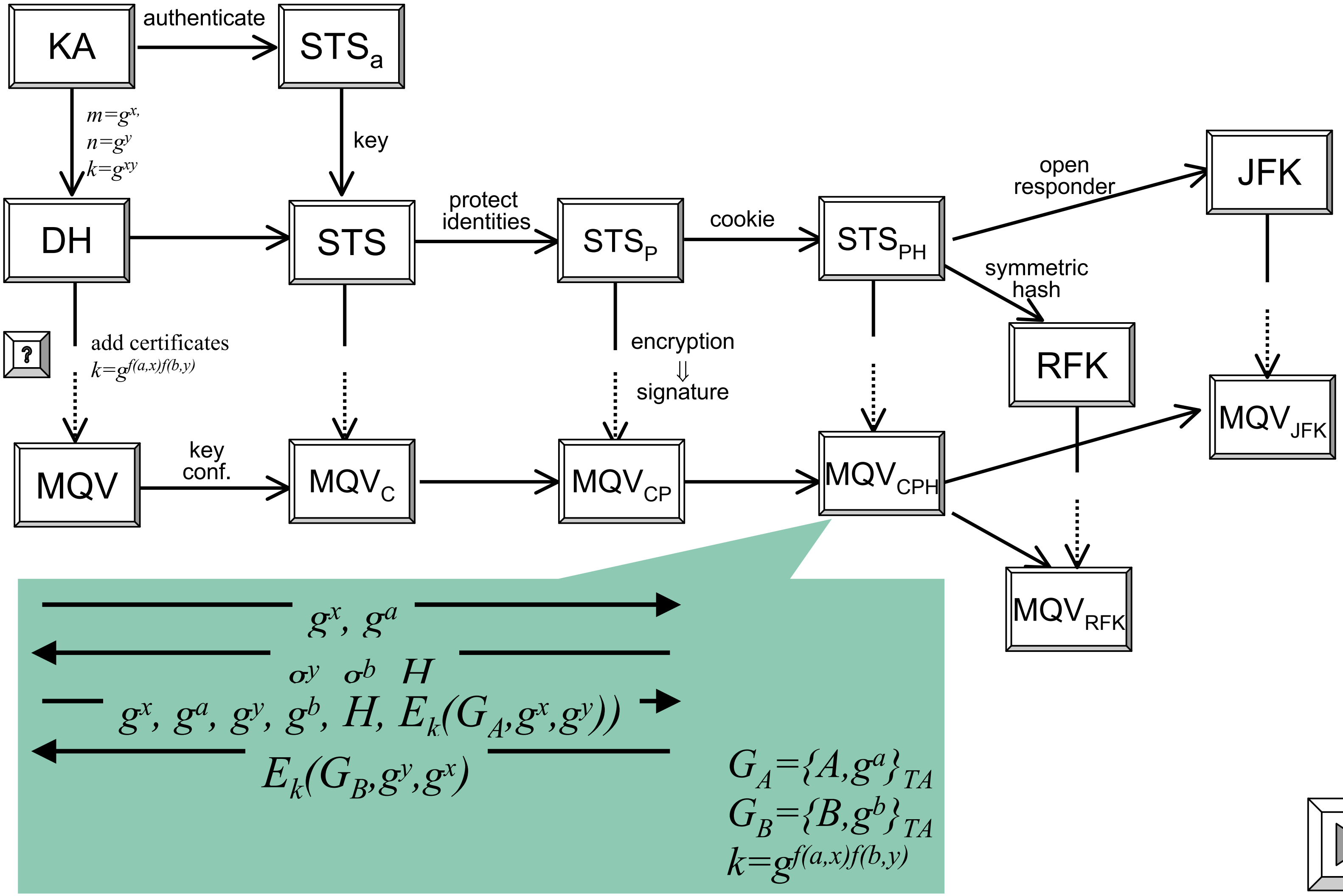
$G_A, E_k(g^x, g^y) \longrightarrow$

$G_A=\{A,g^a\}_{TA}$
$G_B=\{B,g^b\}_{TA}$
$k=g^{f(a,x)f(b,y)}$

MQV refinements



MQV refinements



$$\xrightarrow{g^x,\ g^a}$$

$$\xleftarrow{\sigma^y\ \ \sigma^b\ \ H}$$

$$\xrightarrow{g^x,\ g^a,\ g^y,\ g^b,\ H,\ E_k(G_A,g^x,g^y))}$$

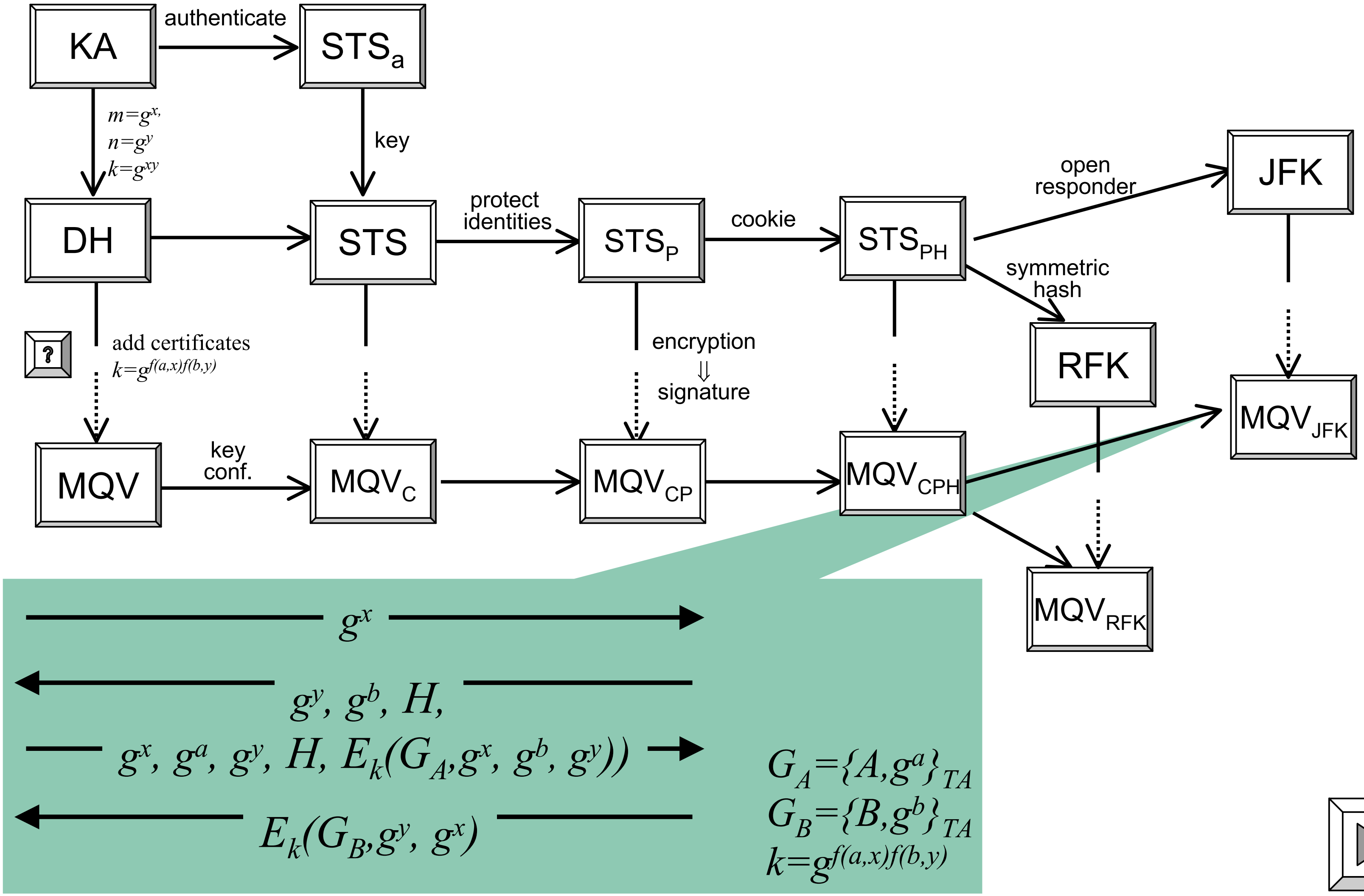
$$\xleftarrow{E_k(G_B,g^y,g^x)}$$

$G_A=\{A,g^a\}_{TA}$

$G_B=\{B,g^b\}_{TA}$

$k=g^{f(a,x)f(b,y)}$

MQV refinements



$$\xrightarrow{\quad g^x \quad}$$

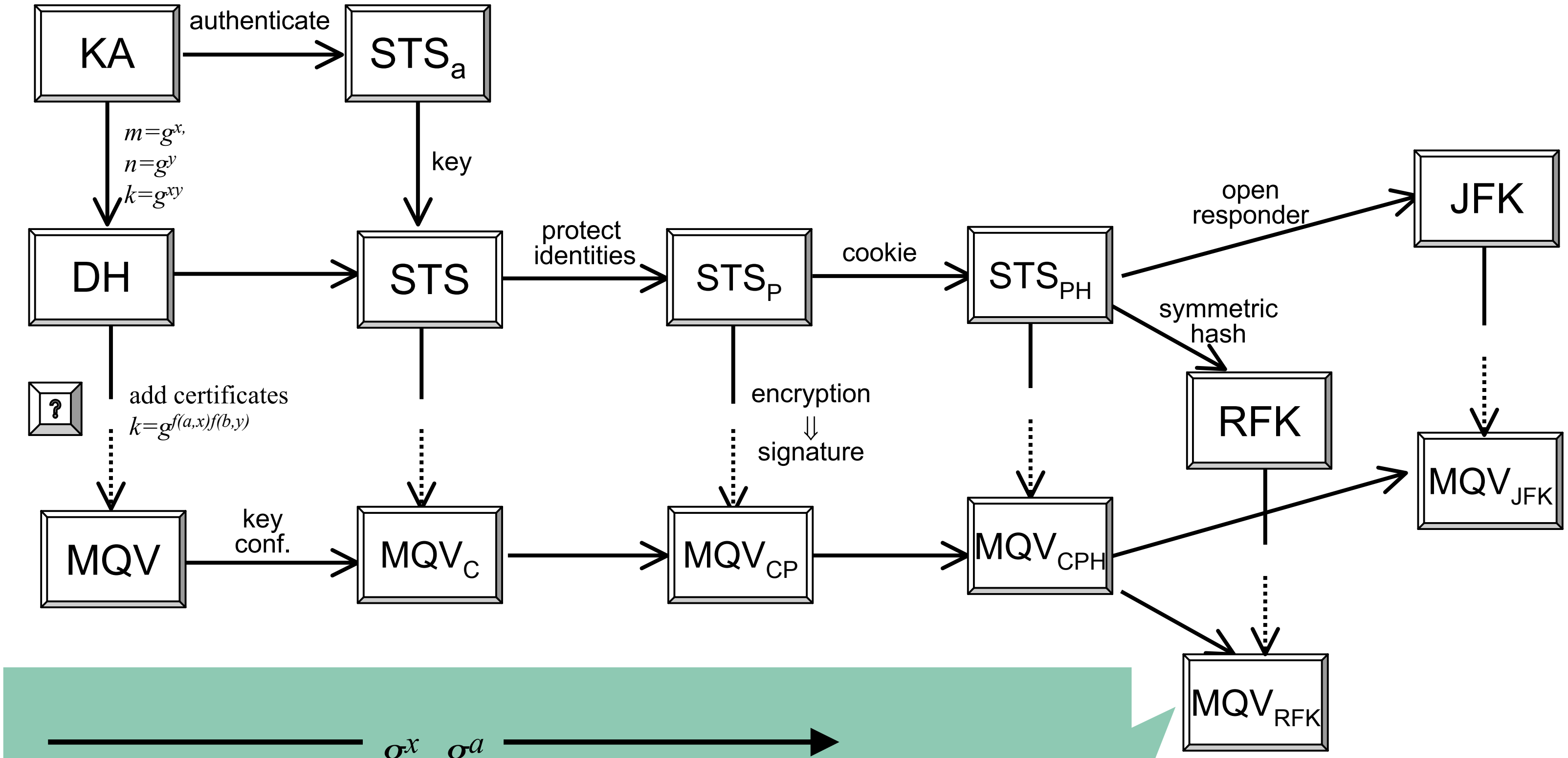
$$\xleftarrow{\quad g^y,\ g^b,\ H, \quad}$$

$$\xrightarrow{\quad g^x,\ g^a,\ g^y,\ H,\ E_k(G_A, g^x,\ g^b,\ g^y)) \quad}$$

$$\xleftarrow{\quad E_k(G_B, g^y,\ g^x) \quad}$$

$G_A=\{A,g^a\}_{TA}$
$G_B=\{B,g^b\}_{TA}$
$k=g^{f(a,x)f(b,y)}$

MQV refinements



$$\xrightarrow{\quad g^x,\ g^a \quad}$$

$$\xleftarrow{\quad g^y,\ g^b,\ H, \quad}$$

$$\xrightarrow{\quad g^x,\ g^a,\ g^y,\ g^b,\ H,\ E_k(G_A,g^x,g^y),\ \#(I) \quad}$$

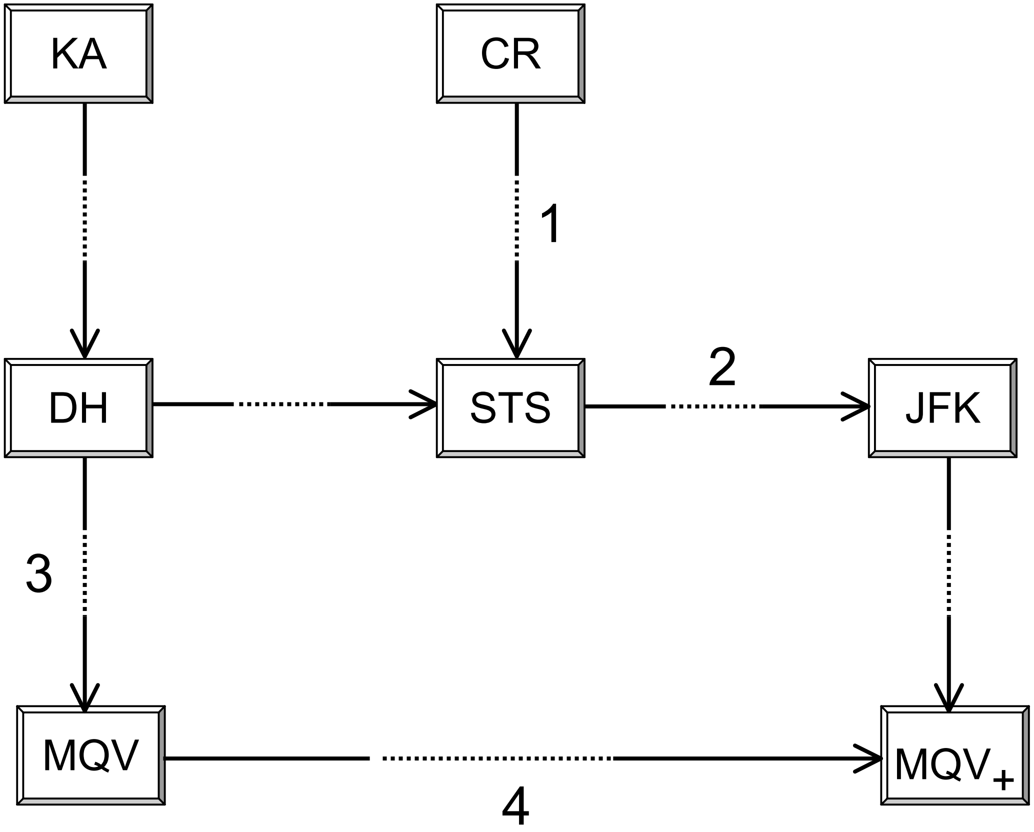
$$\xleftarrow{\quad E_k(G_B,g^y,g^x),\ \#(R) \quad}$$

$G_A=\{A,g^a\}_{TA}$

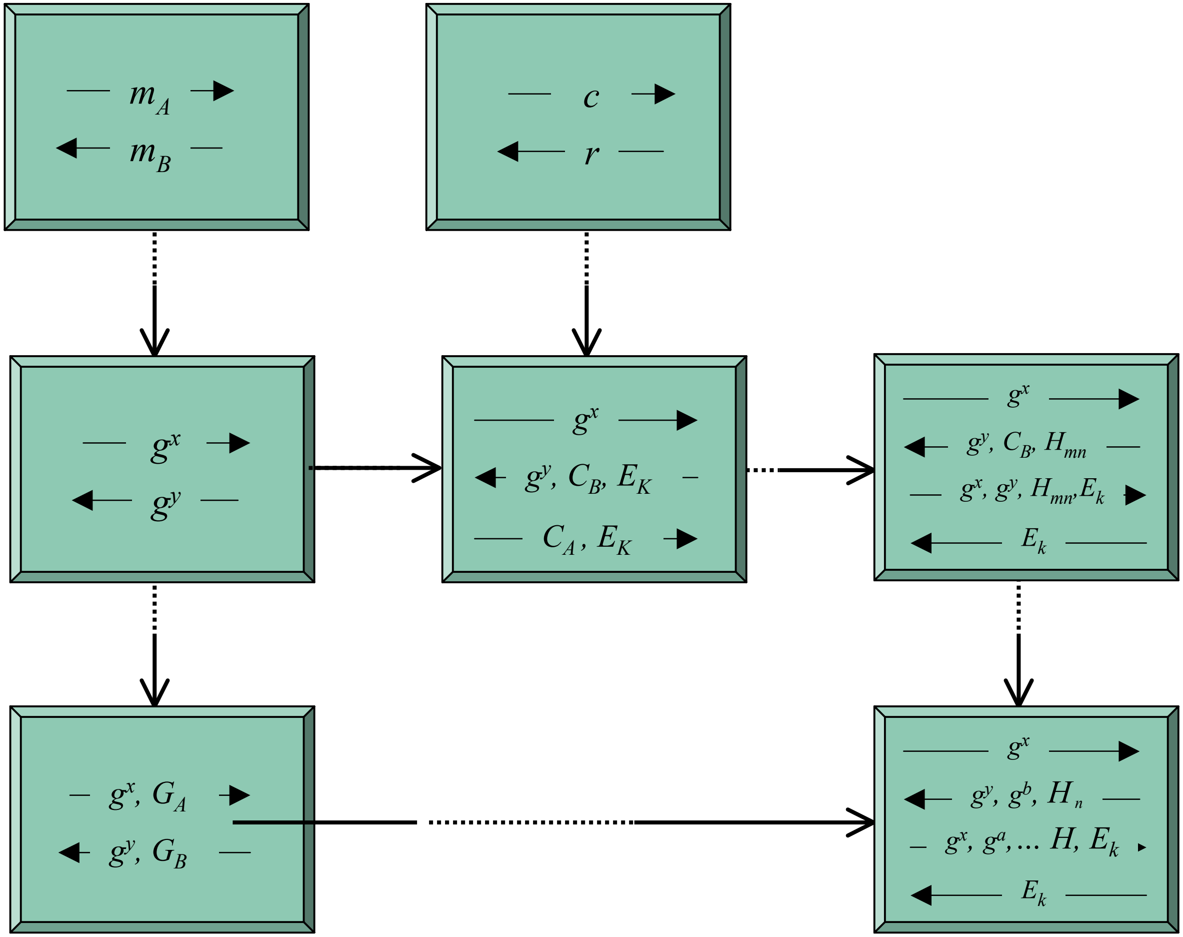
$G_B=\{B,g^b\}_{TA}$

$k=g^{f(a,x)f(b,y)}$

Summary



Summary



m_A

m_B

c

r

g^x

g^y

g^x

g^y, C_B, E_K

C_A, E_K

g^x

g^y, C_B, H_{mn}

g^x, g^y, H_{mn}, E_k

E_k

g^x, G_A

g^y, G_B

g^x

g^y, g^b, H_n

$g^x, g^a, \ldots H, E_k$

E_k

Future work

- Logic
- Tool support
- Populate libraries
- Adaptable protocols
  - runtime reconfiguration under DoS