The Exact Price for Unconditionally Secure Asymmetric Cryptography

Renato Renner

ETH Zürich, Switzerland

Stefan Wolf

Université de Montréal, Canada

Overview

- Motivation
  - What is an asymmetrically secure secret key?
  - What is it good for?
- Main results
  - What is the price for an asymmetrically secure secret key?
  - What is the price for asymmetric security?

Asymmetric security

Facts about unconditionally secure message transmission

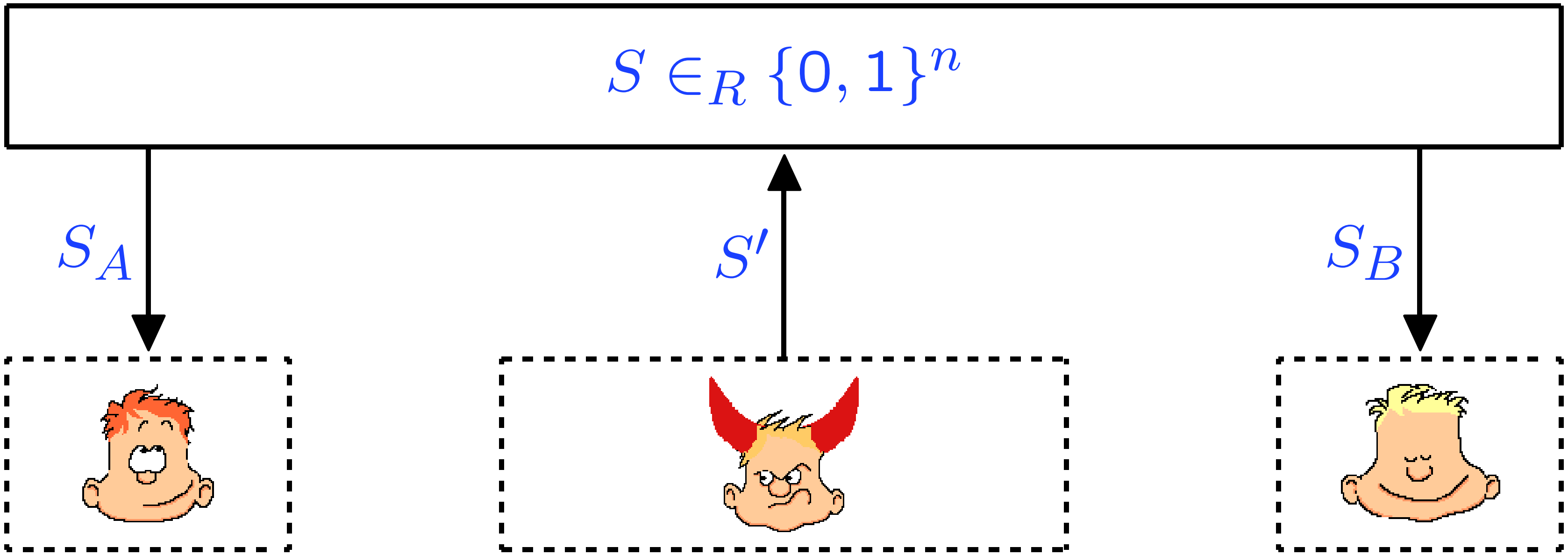
- “secure key” $+$ “insecure channel” $\Rightarrow$ “secret channel”
  (one-time pad)
- “secure key” $+$ “insecure channel” $\Rightarrow$ “authentic channel”
  (message authentication, e.g., based on two-universal hashing)

Consequently

- “secure key” $+$ “insecure channel” $\Rightarrow$ “secure channel”

Asymmetric security

Symmetrically secure secret key

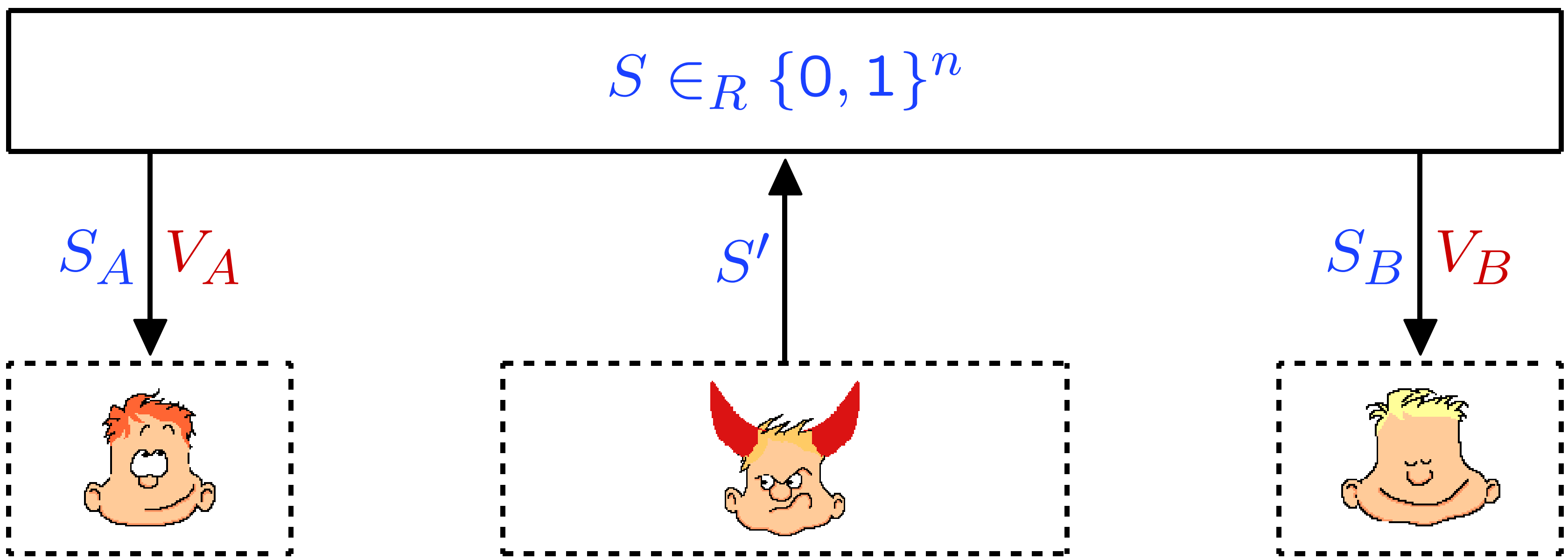


Requirement

- $S_A = S_B = S$ (where S is ind. of adversary's knowledge).

Asymmetric security

Symmetrically secure secret key

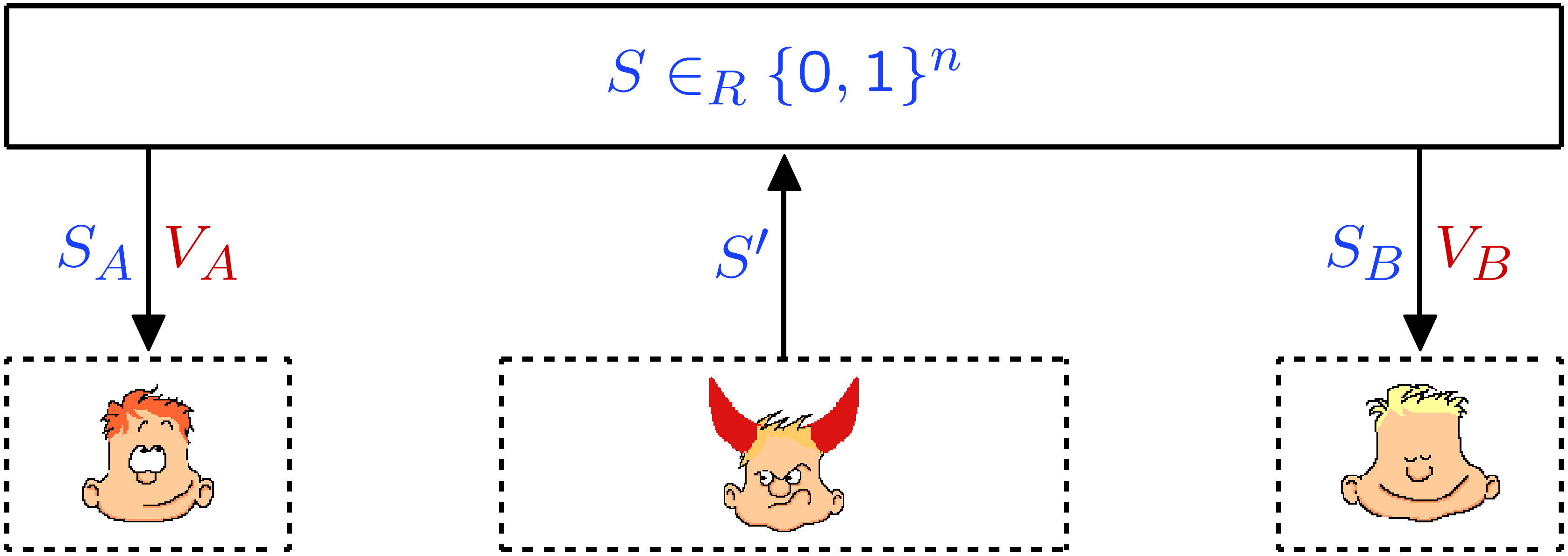


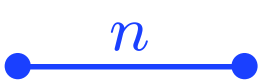
Requirements

- $(V_A = \text{valid}) \vee (V_B = \text{valid}) \Longrightarrow S_A = S_B = S$ (S ind. of S').
- $S' = \perp \Longrightarrow (V_A = \text{valid}) \wedge (V_B = \text{valid})$.

Asymmetric security

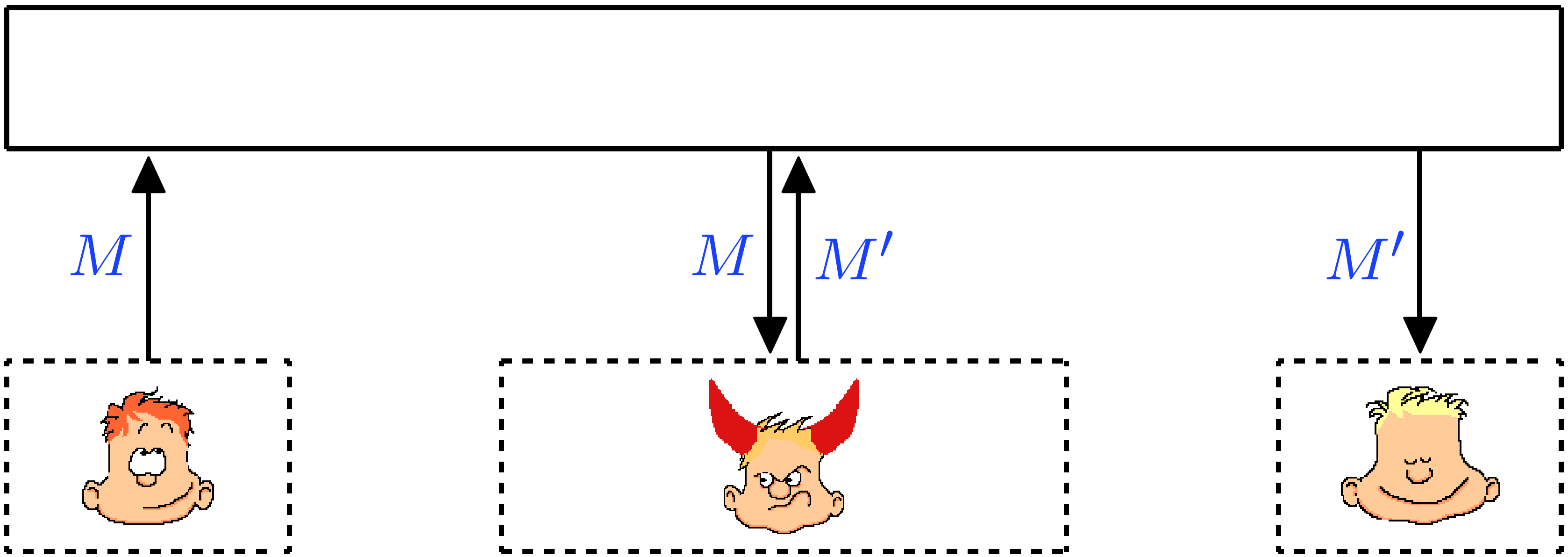
Symmetrically secure secret key



Notation: "  "

Asymmetric security

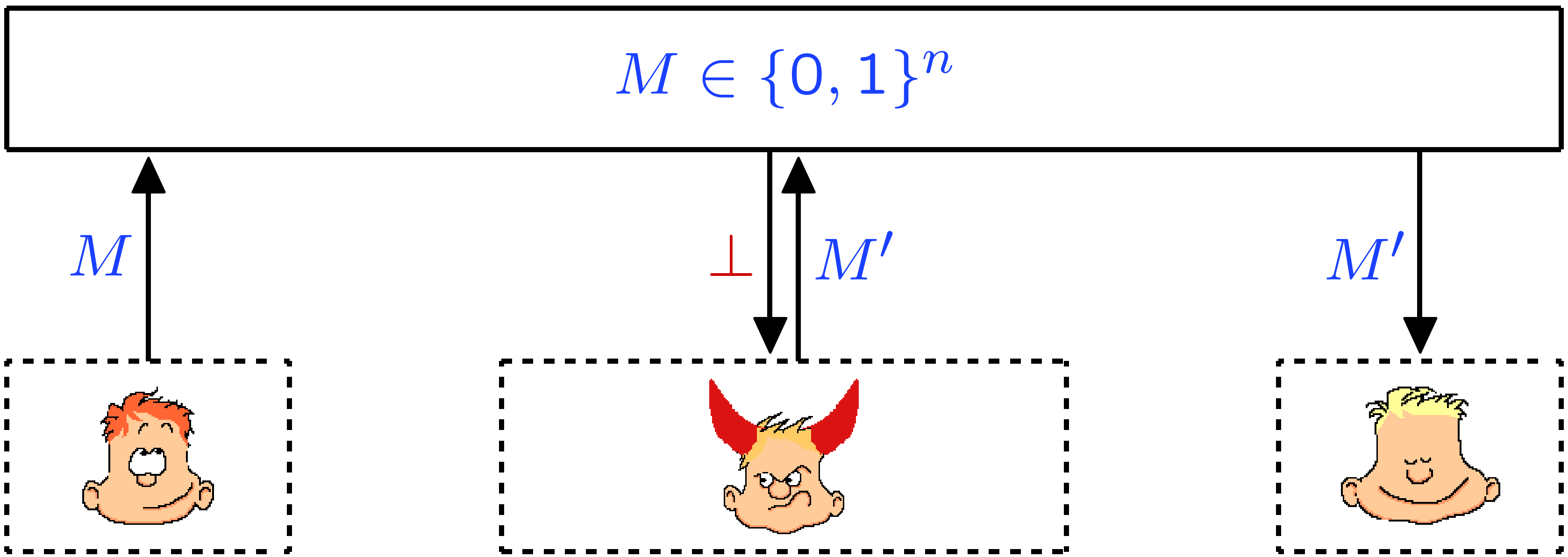
Insecure communication channel



Notation: “ $\longrightarrow$ ”

Asymmetric security

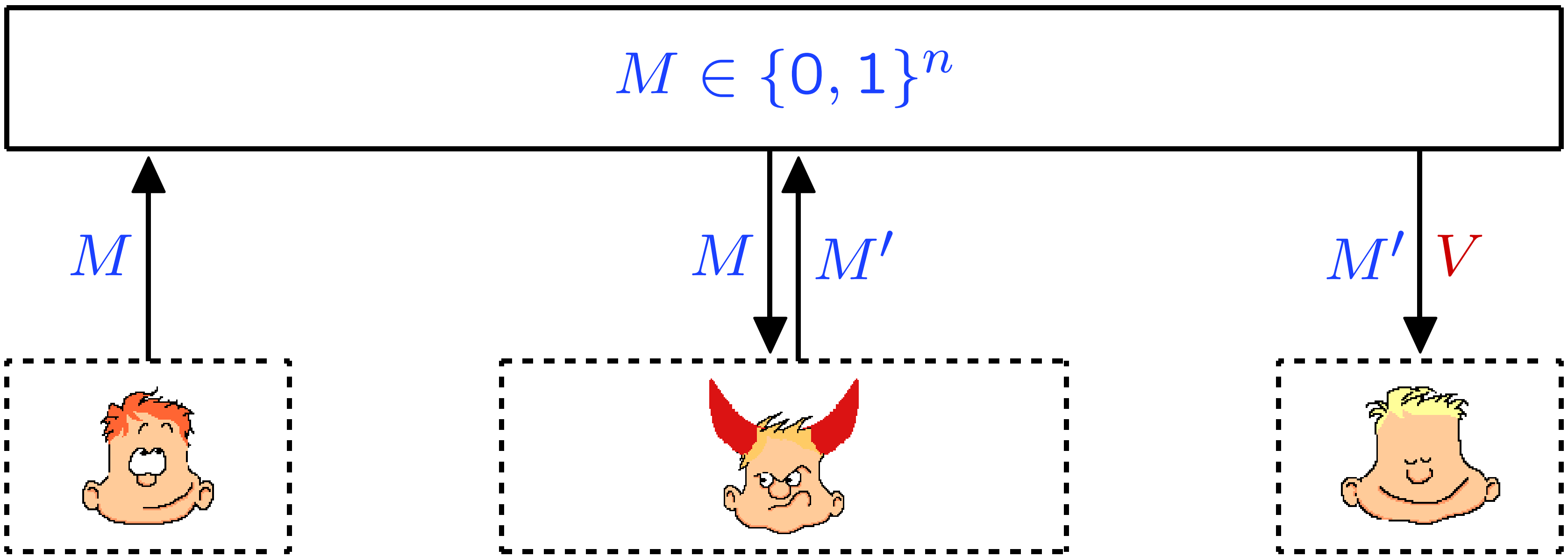
Secret channel



Notation: " 

"

Authentic channel

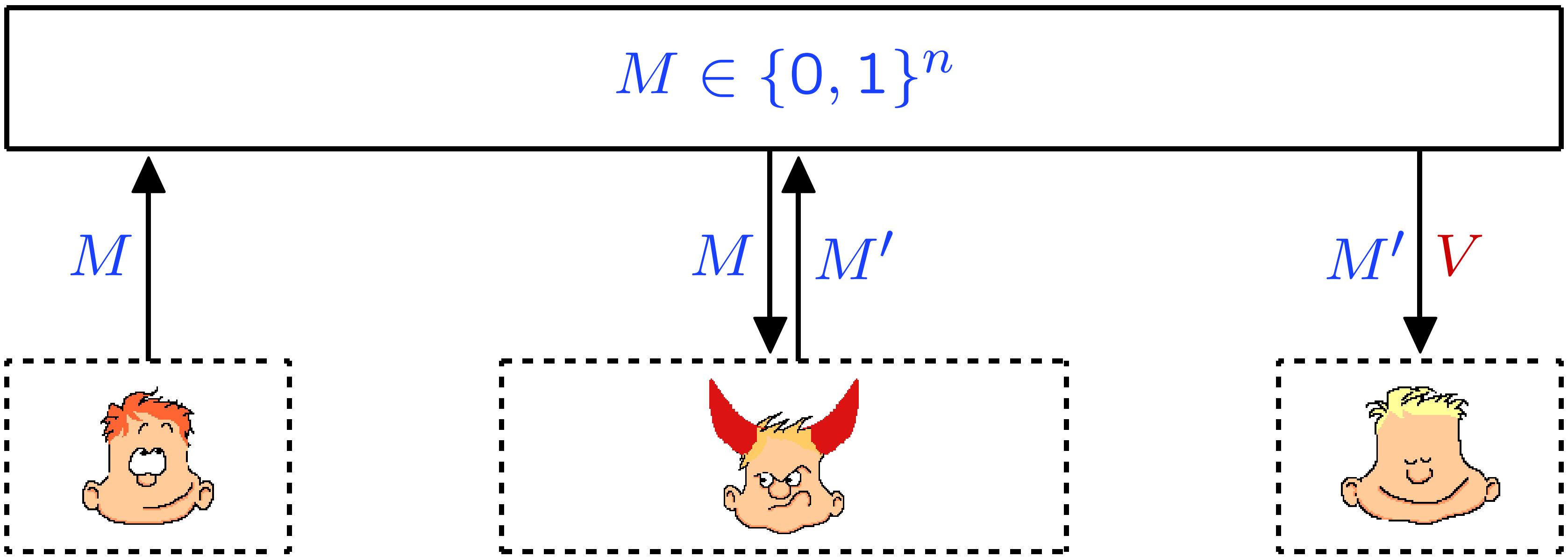


Requirements

- $V = \text{valid} \implies M' = M$
- $M' = \perp \implies V = \text{valid}$.

Asymmetric security

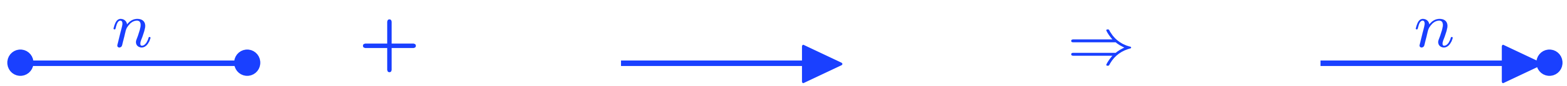
Authentic channel



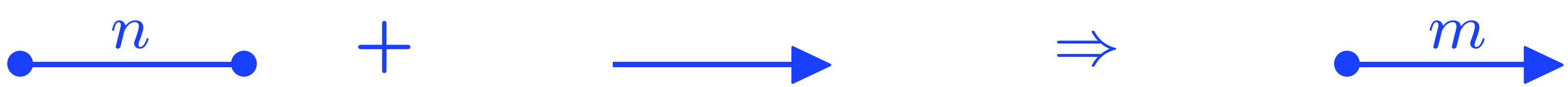
Notation: " $\xrightarrow{n}$ "

Facts about unconditionally secure message transmission

- “secure key” $+$ “insecure channel” $\Rightarrow$ “secret channel”



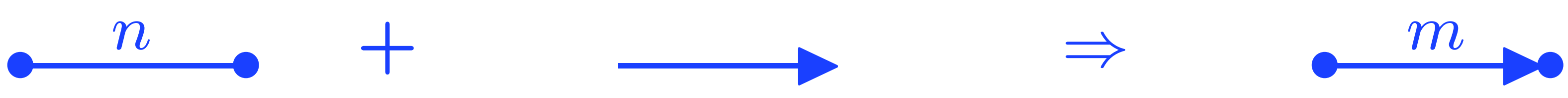
- “secure key” $+$ “insecure channel” $\Rightarrow$ “authentic channel”



(where $m \gg n$)

Consequently

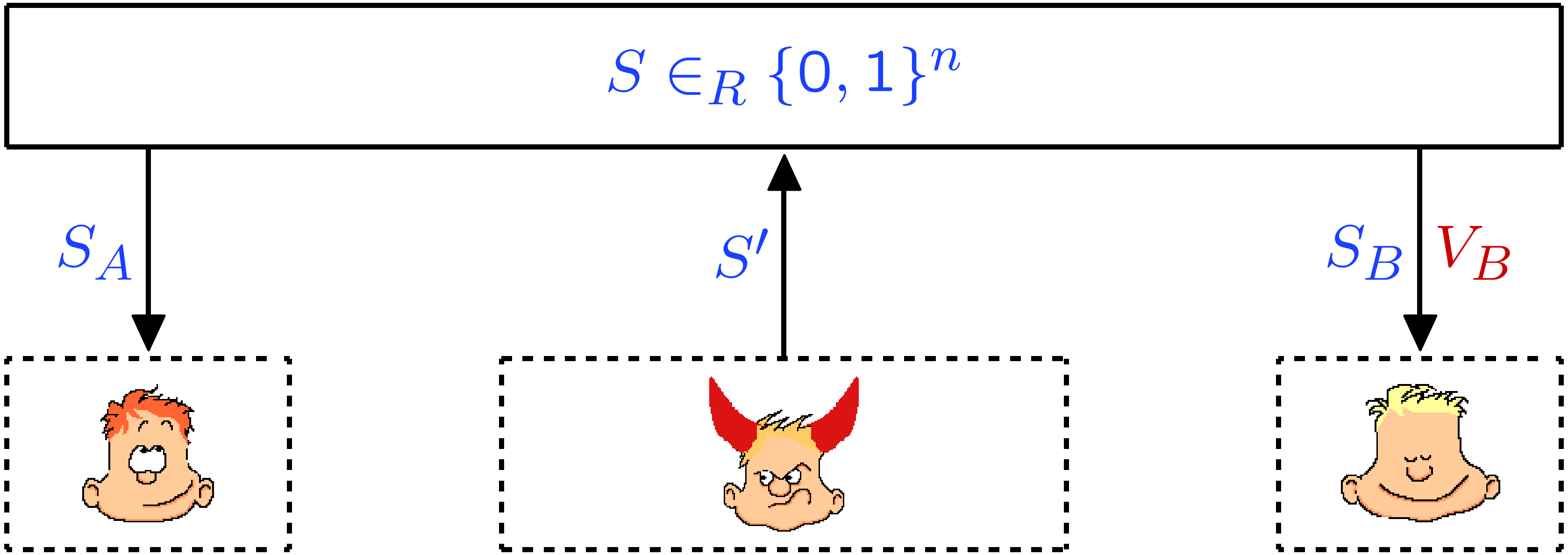
- “secure key” $+$ “insecure channel” $\Rightarrow$ “secure channel”



(where $m \approx n$)

Asymmetric security

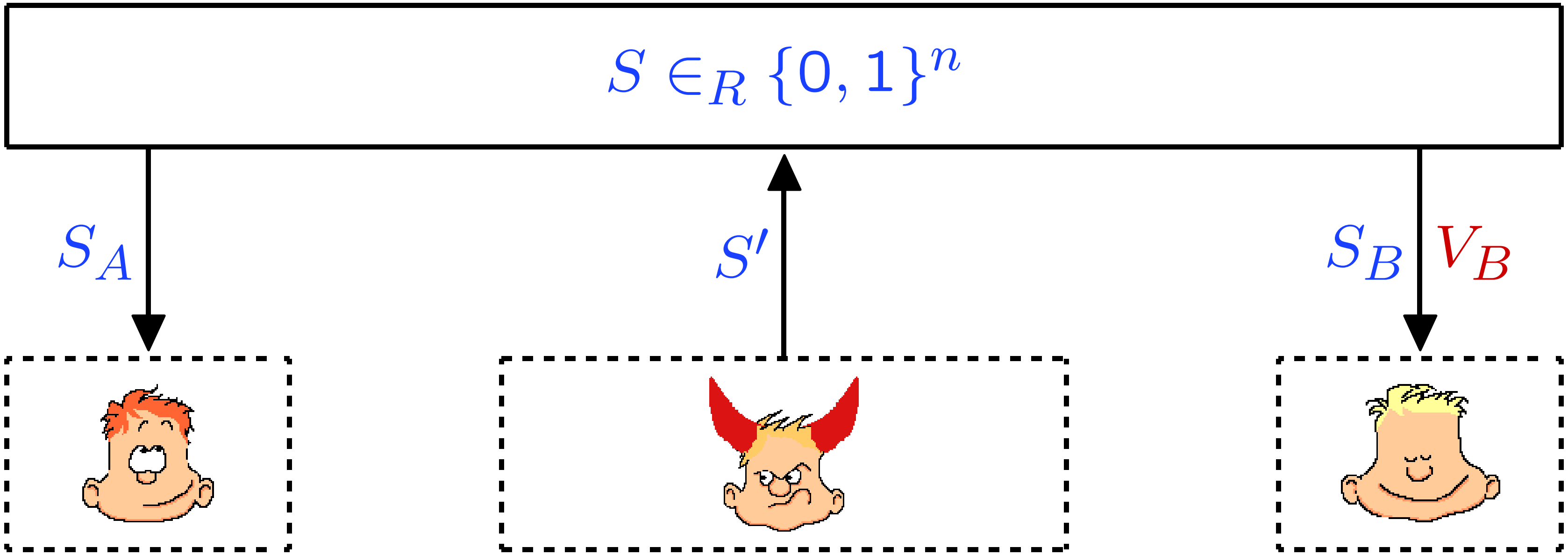
Asymmetrically secure secret key



Requirements

- $V_B = \text{valid} \Longrightarrow S_A = S_B = S$ (S ind. of S').
- $S' = \perp \Longrightarrow V_B = \text{valid}$.

Asymmetrically secure secret key



Notation: “ 

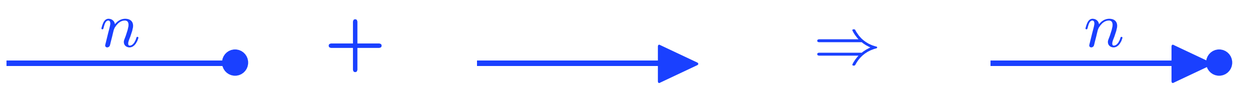
”

Bob knows that

- his key is secret,
- Alice has the same key.

Application of asymmetric keys

- Secret channel from A to B



- Authentic channel from A to B

- Secret channel from B to A

- Authentic channel from B to A

Asymmetric security

Application of asymmetric keys (bidirectional channels)

- Secrecy from A to B / Authenticity from B to A

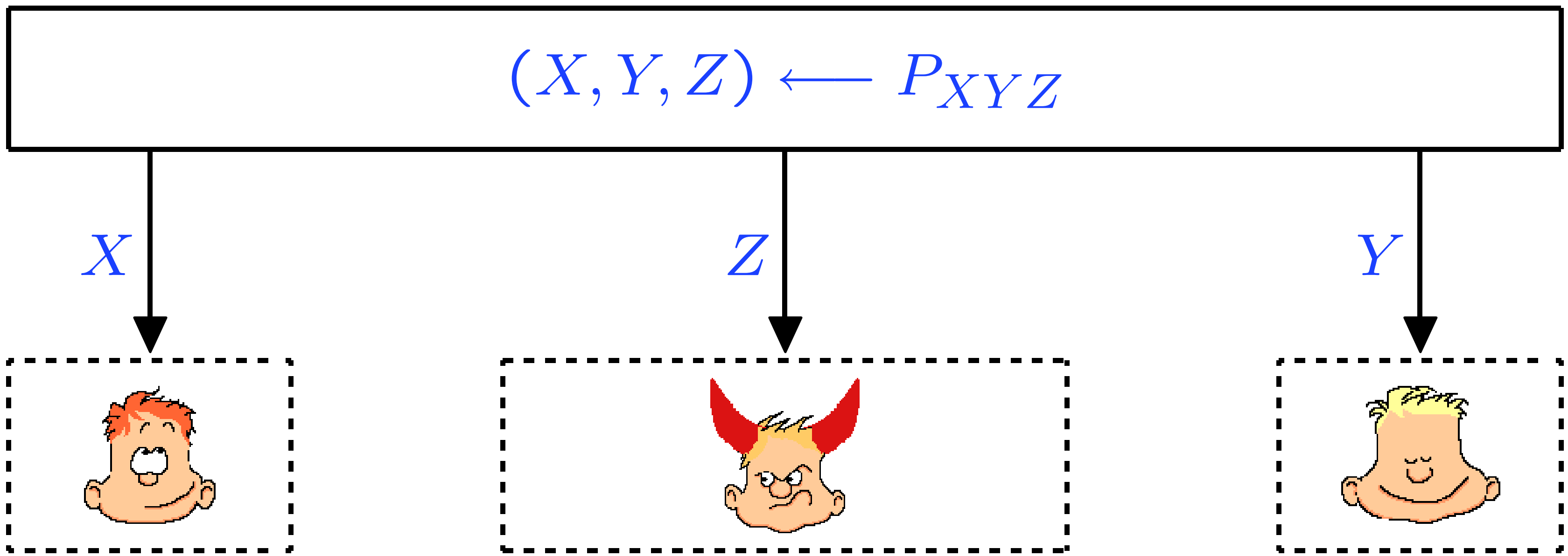
- Authenticity from A to B / Secrecy from B to A

Observation

The price to realize  or  can be much lower than the price to realize  .

Key agreement from correlated information

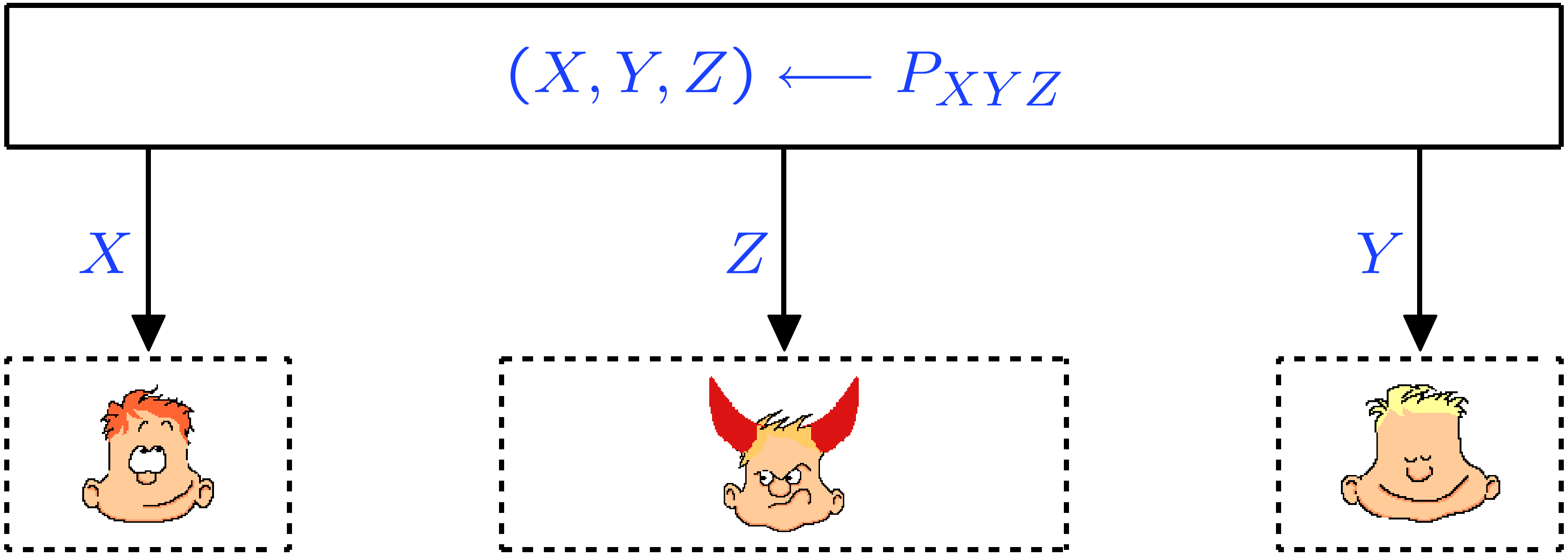
Correlated information



Notation: "P_{XYZ}"

Key agreement from correlated information

Correlated information



Types of correlation

- P_{XYZ} : general case (weakly correlated / only partially secret).
- P_{XXZ} : X and Y identical (fully correlated / only partially secret).
- P_{XY} : $Z = \perp$ (weakly correlated / fully secret).

Key agreement from correlated information

Previous results I

- Key agreement by authentic public discussion [Maurer93]

"correlation"	$+$	"authentic channels"	$\Rightarrow$	"secret key"
$(P_{XYZ})^m$	$+$	$\bullet\!\longrightarrow$ / $\longleftarrow\!\bullet$	$\Rightarrow$	$\bullet\overset{n}{\text{———}}\bullet$

upper bound: $n \leq m \cdot I(X;Y \downarrow Z)$

lower bound: $n \gtrsim m \cdot (I(X;Y) - \min\{I(X;Z), I(Y;Z)\})$.

- Key agreement by non-authentic public discussion

"correlation"	$+$	"insecure channels"	$\Rightarrow$	"secret key"
$(P_{XYZ})^m$	$+$	$\longrightarrow$ / $\longleftarrow$	$\Rightarrow$	$\bullet\overset{n}{\text{———}}\bullet$

characterized by simulatability condition.

Key agreement from correlated information

Previous results II

- *Privacy amplification* over authentic channel

“insecure string” $+$ “authentic channel” $\Rightarrow$ “secret key”

P_{XXZ} $+$  $\Rightarrow$ 

key length: $n \gtrsim H_\infty(X|Z)$ [BBR88, BBCM95].

$(H_\infty(V) := -\log_2 \max_v P_V(v).)$

- *Privacy amplification* over non-authentic channel

“insecure string” $+$ “insecure channel” $\Rightarrow$ “secret key”

P_{XXZ} $+$  $\Rightarrow$ 

key length: $n \gtrsim H_\infty(X|Z)$ [RenWol03].

Key agreement from correlated information

Main result: Arbitrary correlation / non-authentic channel

- Generation of asymmetric key

"correlation"	$+$	"insecure channel"	$\Rightarrow$	"secret key"
P_{XYZ}	$+$	$\longleftrightarrow$	$\Rightarrow$	$\bullet\!\overset{n}{\text{———}}$

key length: $n \gtrsim H_\infty(Y|Z) - H_0(Y|X)$.

$(H_0(V) := \log_2 |\{v : P_V(v) > 0\}|.)$

- Generation of symmetric key

"correlation"	$+$	"insecure channel"	$\Rightarrow$	"secret key"
P_{XYZ}	$+$	$\longleftrightarrow$	$\Rightarrow$	$\bullet\!\overset{n}{\text{———}}\!\bullet$

key length: $n \gtrsim H_\infty(Y|Z) - H_0(Y|X) - H_0(X|Y)$.

Proof sketch

Theorem

There exists a secret-key agreement protocol SKA such that

P_{XYZ} $+$  $\Rightarrow$ 

for $n \approx H_\infty(Y|Z) - H_0(Y|X)$.

Proof sketch

Known result: Privacy amplification over insecure channel

$P_{YY\bar{Z}}$ $+$  $\Rightarrow$ 

for $m \approx H_\infty(Y|\bar{Z})$.

Proof sketch

Proof sketch

Known result: Privacy amplification over insecure channel

$P_{YY\bar{Z}}$ $+$  $\Rightarrow$ 

for $m \approx H_\infty(Y|\bar{Z})$.

Assume now that Alice holds Y' such that

- if the adversary is passive then $Y = Y'$,
- Bob knows whether $Y = Y'$.

Then

$P_{Y'Y\bar{Z}}$ $+$  $\Rightarrow$ 

for $m \approx H_\infty(Y|\bar{Z})$.

Proof sketch

Goal

Find *information reconciliation* protocol IR for transformation

$$P_{XYZ} \ + \quad \longleftrightarrow \quad \Rightarrow \quad P_{Y'Y\bar{Z}}$$

such that

- if the adversary is passive then $Y = Y'$,
- Bob knows whether $Y = Y'$,
- $H_\infty(Y|\bar{Z}) \gtrapprox H_\infty(Y|Z) - H_0(Y|X)$

  ($\bar{Z}$: knowledge of adversary after execution of protocol IR).

Proof sketch

Protocol IR (information reconciliation)

Alice		Bob
$X \in \{0,1\}^n$		$Y \in \{0,1\}^n$
		$H \in_R \mathcal{H}$ $H : \{0,1\}^n \rightarrow \{0,1\}^d$
	$\xleftarrow{\quad H, H(Y) \quad}$	
$Y' \in \mathcal{Y}_X$ with $H(Y') = H(Y)$		

For $d \approx H_0(Y|X)$

- $Y' = Y$ with high probability,
- $H_\infty(Y|ZC) \gtrsim H_\infty(Y|Z) - H_0(Y|X)$.

Proof sketch

Protocol IR' (information reconciliation / check)

Alice		Bob
$X \in \{0,1\}^n$		$Y \in \{0,1\}^n$
		$H \in_R \mathcal{H}$ $H : \{0,1\}^n \to \{0,1\}^d$
	$\xleftarrow{\;H, H(Y)\;}$	
$Y' \in \mathcal{Y}_X$ with $H(Y') = H(Y)$		
$R \in_R \mathsf{GF}(2^k)$		
	$\xrightarrow{\;R, p_{Y'}(R)\;}$	
accept Y'		accept Y if $p_{Y'}(R) = p_Y(R)$

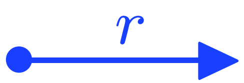
p_y is a function such that $\Pr[p_y(R) = p_{y'}(R)]$ small for $y \neq y'$

(e.g., a polynomial of degree n/k over $\mathsf{GF}(2^k)$ depending on y).

Proof sketch

Lemma (interactive authentication) [RenWol03].

Let $r > 0$. If $H_\infty(Y|\bar{Z})$ sufficiently large then AUTH realizes

$P_{YY\bar{Z}}$ $+$  $\Rightarrow$  .

Idea

Show that AUTH remains secure if $Y' \neq Y$.

Proof sketch

Lemma (interactive authentication) [RenWol03].

Let $r > 0$. If $H_\infty(Y|\bar{Z})$ sufficiently large then AUTH realizes

$$P_{Y'Y\bar{Z}} + \longleftrightarrow \quad \Rightarrow \quad \bullet\!\xrightarrow{\;r\;} \qquad \text{(for } Y' = Y\text{).}$$

Idea

Setting:

- Alice holds Y'.
- Bob holds Y.
- Eve holds $\bar{Z}$ such that $H_\infty(Y|\bar{Z})$ sufficiently large.
- Eve is allowed to arbitrarily interact with Alice and Bob.

To prove: Bob never accepts a message M' which is not sent by Alice.

Asymmetric result

There exists a secret key agreement protocol SKA such that

$P_{XYZ} \; +$

where $n \gtrapprox H_\infty(Y|Z) - H_0(Y|X) \quad (*)$.

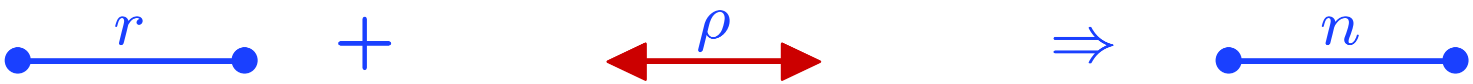
Remarks

- SKA only depends on $H_\infty(Y|Z)$ and $H_0(Y|X)$.
- The resulting key size is optimal w.r.t. $(*)$.
- SKA works for all distributions $P_{X'Y'Z'}$ such that $\delta(P_{XYZ}, P_{X'Y'Z'})$ is small for some P_{XYZ} satisfying $(*)$.
- If $P_{XYZ} = P^m_{\bar{X}\bar{Y}\bar{Z}}$ (for large m) then $(*)$ reduces to $n \approx m \cdot (H(\bar{Y}|\bar{Z}) - H(\bar{Y}|\bar{X}))$ [CsiKoe78].

Applications in quantum cryptography

- Quantum key agreement (key extension)

“short SK” $+$ “quantum channel” $\Rightarrow$ “long SK”

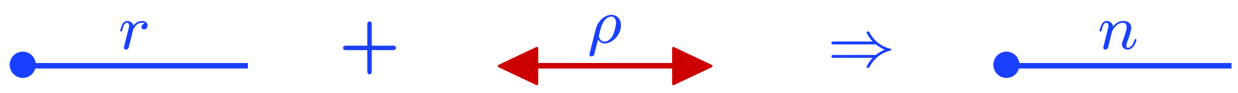


where $r \ll n$.

Concluding remarks

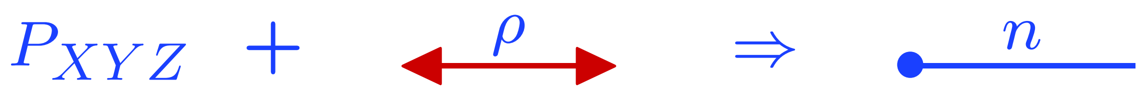
Applications in quantum cryptography

- Asymmetric quantum key extension



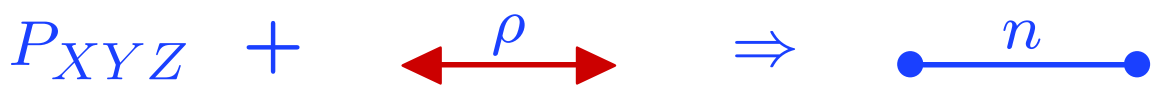
(where $r \ll n$)

- Correlation is sufficient ...



(for $H_\infty(Y|Z) - H_0(Y|X) > 0$)

- ... even for the generation of a symmetric key



(for $H_\infty(Y|Z) - H_0(Y|X) - H_0(X|Y) > 0$).

Questions?