
# *Sicherheit:*
# *Fragen und Lösungsansätze*

im Wintersemester 2012 / 2013

Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Teil 9: Some Further Cryptographic Protocols
v. 27.01.2013

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# Themen der Vorlesung





©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# Covert commitments

- ***committing*** **:**
  the *committer* discretionarily selects some value $v_{com}$
  and commits to this value, in a covert form regarding the *receiver*
- ***revealing*** **:**
  the *committer* reveals a value $v_{show}$ to the *receiver*,
  who in turn either accepts or rejects it as the committed value
- ***binding property*** (combined *correctness* and *unforgeability* property)**:**

  for all values $v_{com}$:

  if the committer enters the revealing phase at all,
  then the receiver accepts the revealed value $v_{show}$

  if and only if it is the committed value $v_{com}$
- ***secrecy property*** (after committing and before revealing)**:**

  for all values $v_{com}$,

  the receiver cannot “determine”
  the committed value $v_{com}$ from the covert form

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# Secret sharing

- ***distributing*** **:**
  the *owner* of the secret *v* computes *shares* $s_1,\ldots, s_n$ and distributes them to appropriate *receivers*
- ***combining*** **:**
  for some threshold $t \leq n$, *t* (or more) *receivers* collect their shares $s_{i_1},\ldots,s_{i_t}$ and use them to recover the secret
- ***correctness property*****:**

  for all values *v* :
  the receivers succeed in determining the secret value *v*
  from any set of *t* distinct shares $s_{i_1},\ldots,s_{i_t}$
- ***secrecy property*****:**

  for all values *v* :
  the receivers cannot “determine” the secret value *v*
  from any set of *t*-1 shares

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

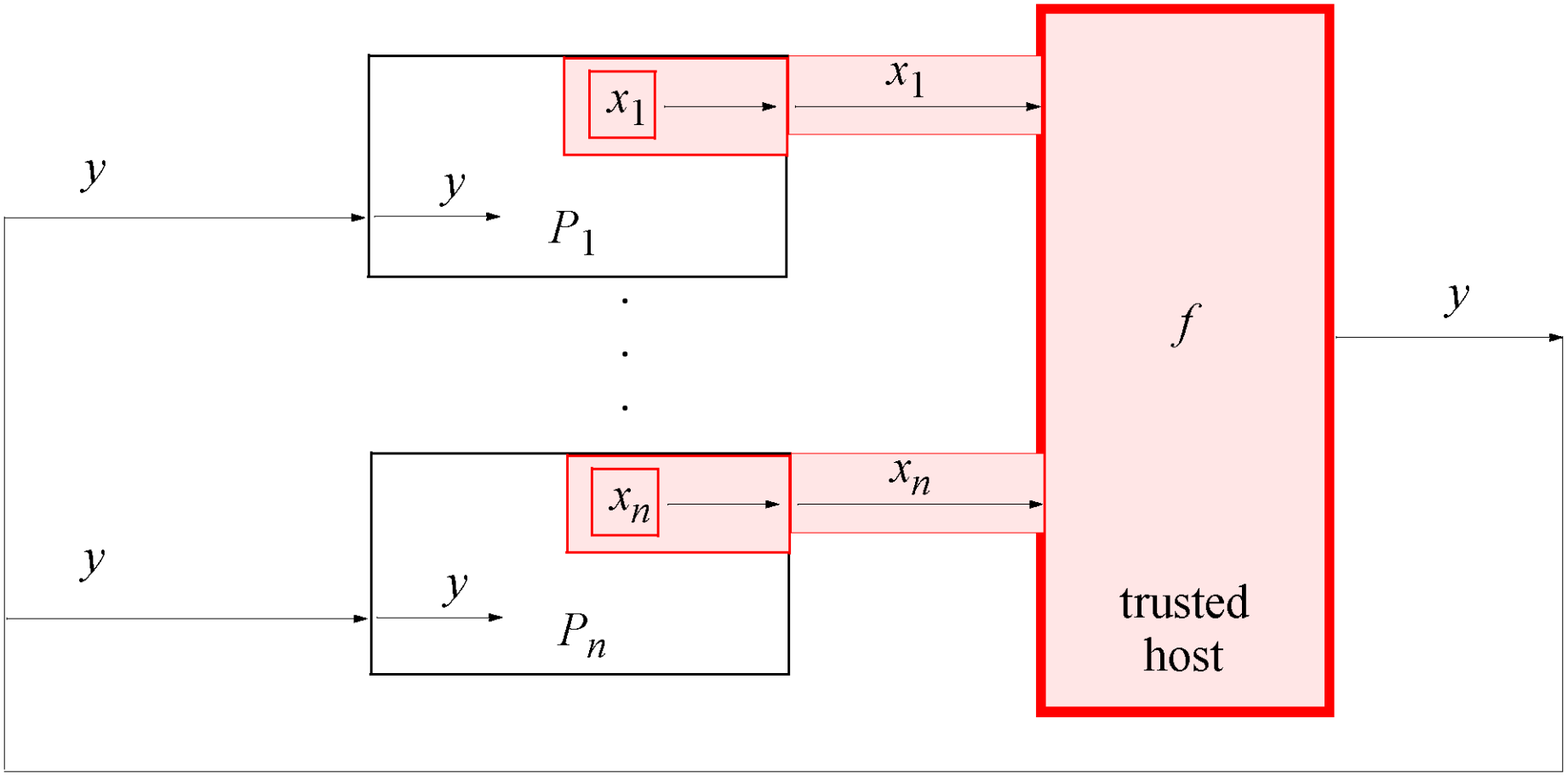
# Multiparty computations

- multiparty computations address a very general situation of *cooperation in the presence of threats* between $n$ parties $P_i$
- parties aim at jointly computing the value $y$ of some agreed $n$-ary function $f$:
  - each $P_i$ secretly provides an argument $x_i$
  - at the end, each $P_i$ knows the computed value $y = f(x_1,\ldots, x_n)$
  - no $P_i$ learns anything new about the other parties' arguments
- ***correctness property*** (with threshold $t$)**:**
  for all inputs $x_1,\ldots, x_n$ of the parties $P_1,\ldots, P_n$ , respectively, with $n > 2$,
  if the adversary is formed by at most $t$ attacking parties (a strict minority),
  then each of the honest parties obtains $f(x_1,\ldots, x_n)$ as the final result
- ***secrecy property*** (with threshold $t$)**:**
  for all inputs $x_1,\ldots, x_n$ of the parties $P_1,\ldots, P_n$ , respectively, with $n > 2$,
  an adversary formed by at most $t$ attacking parties (a strict minority)
  cannot "determine" any of the secret inputs of the honest parties

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

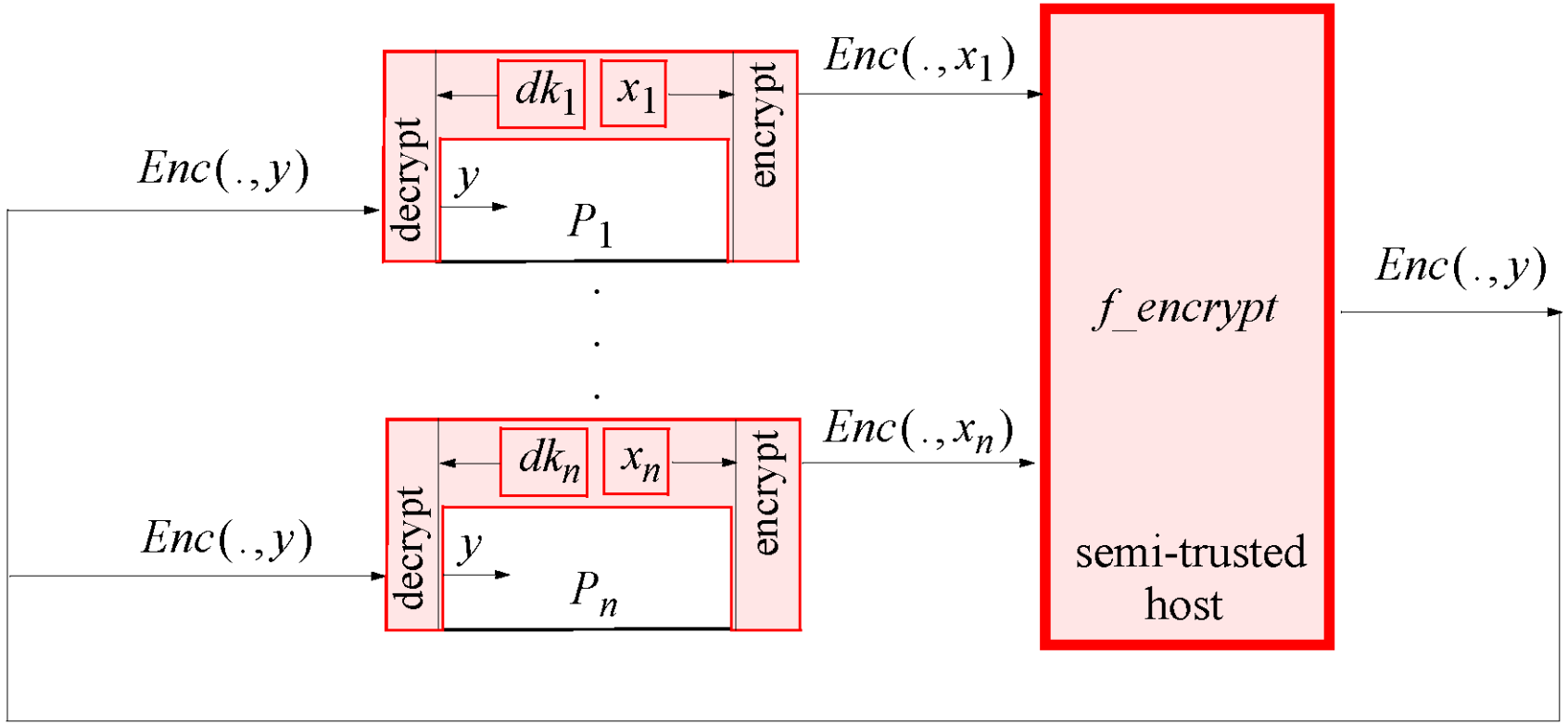
# A trusted host with private input channels





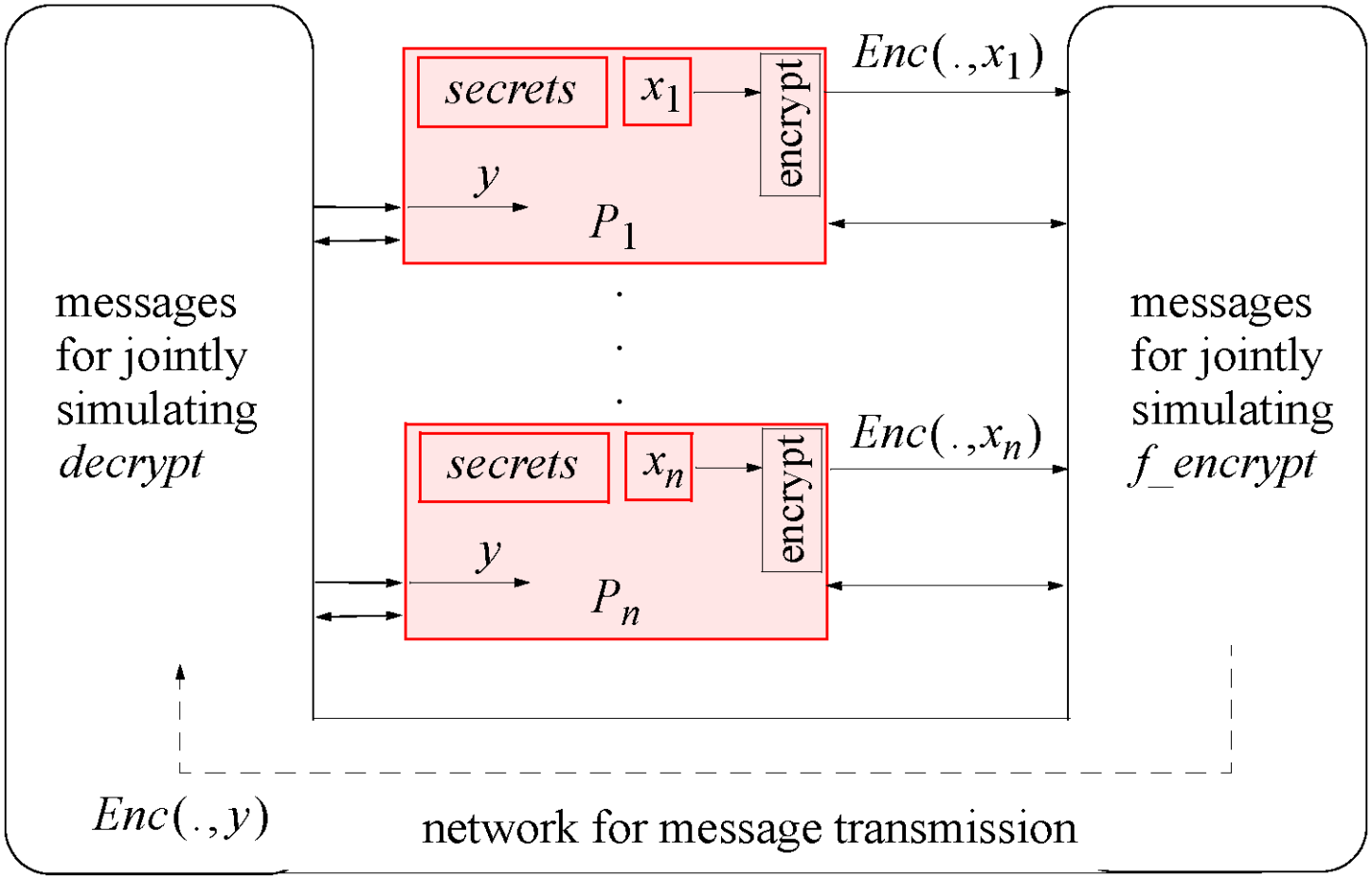

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# A semi-trusted host operating on ciphertexts




©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# Parties with protected local operations and message transmissions




©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems

# A combined correctness and secrecy property (with threshold t)

whatever violations of correctness and secrecy
can be achieved in the model of
parties cooperating by protected local operations and message transmissions

can also (inevitably) happen in the trusted-host model,
and thus, in particular,
without observing messages of the honest parties at all

©2009 Springer-Verlag Berlin Heidelberg / ©2010 Joachim Biskup TU Dortmund / Jan Jürjens : Security in Computing Systems