

Universally Composable Symbolic Analysis of Diffie-Hellman and Certification

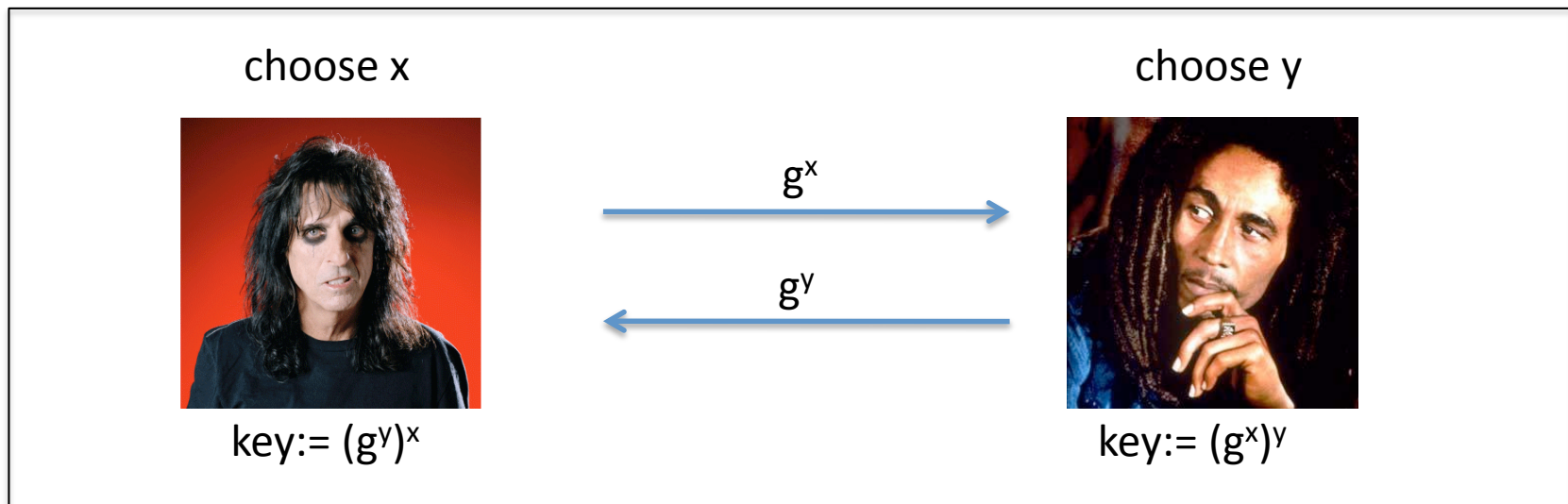
Ran Canetti and Sebastian Gajek

School of Computer Science

Tel Aviv University, Israel

Diffie-Hellman Key Exchange (DHKE)

- Alice and Bob want to establish a session key
- Important tool for other primitives (e.g. secure channels, hybrid encryption)



[Diffie-Hellman, '76]

The Symbolic Obstacles

- **Algebraic properties** of modular exponentiation

$$a = b^c \pmod n$$

- Commutativity in Z_n^*

$$(g^{p(x)})^{q(y)} = ((g^{q(y)})^{p(x)}) \pmod n$$

- Associativity in Z_n^*

$$(g^{p(x)}) (g^{q(x)}) = (g^{p(x)+q(y)}) \pmod n$$

- Inverse in Z_n^*

$$(g^{p(x)})^{-p(x)} = g^1 \pmod n$$

- Pairing, ...

**HOW TO CAPTURE THE PROPERTIES OF
DIFFIE-HELLMAN IN THE SYMBOLIC MODEL?**

Previous Work

[H. Comon-Lundh, R. Treinen: *Easy Intruder Deductions*. *Verification: Theory and Practice 2003*], [H. Comon-Lundh, V. Shmatikov: *Intruder Deductions, Constraint Solving and Insecurity Decision in Presence of Exclusive or*. *LICS 2003*], [Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani: *Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents*. *FSTTCS 2003*], [Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani: *An NP Decision Procedure for Protocol Insecurity with XOR*. *LICS 2003*], [M. Abadi, V. Cortier: *Deciding Knowledge in Security Protocols Under Equational Theories*. *ICALP 2004*], [C. Lynch, C. Meadows: *Sound Approximations to Diffie-Hellman Using Rewrite Rules*. *ICICS 2004*], [M. Abadi, V. Cortier: *Deciding Knowledge in Security Protocols under (Many More) Equational Theories*. *CSFW 2005*], [H. Comon-Lundh, S. Delaune: *The Finite Variant Property: How to Get Rid of Some Algebraic Properties*. *RTA 2005*], [P. Lafourcade, D. Lugiez, R. Treinen: *Intruder Deduction for AC-Like Equational Theories with Homomorphisms*. *RTA 2005*], [J. Millen, V. Shmatikov: *Symbolic protocol analysis with an Abelian group operator or Diffie-Hellman exponentiation*. *Journal of Computer Security 13(3)*], [S. Delaune, P. Lafourcade, D. Lugiez, R. Treinen: *Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or*. *ICALP (2) 2006*], [M. Abadi, V. Cortier: *Deciding knowledge in security protocols under equational theories*. *Theor. Comput. Sci. 367(1-2)*], [S. Escobar, C. Meadows, J. Meseguer: *Equational Cryptographic Reasoning in the Maude-NRL Protocol Analyzer*. *ENTCS 171(4)*], [S. Bursuc, H. Comon-Lundh, S. Delaune: *Associative-Commutative Deducibility Constraints*. *STACS 2007*], [P. Lafourcade, D. Lugiez, R. Treinen: *Intruder deduction for the equational theory of Abelian groups with distributive encryption*. *Inf. Comput. 205(4)*], [M. Arnaud, V. Cortier, S. Delaune: *Combining Algorithms for Deciding Knowledge in Security Protocols*. *FroCos 2007*], [V. Cortier, S. Delaune: *Deciding Knowledge in Security Protocols for Monoidal Equational Theories*. *LPAR 2007*]

[Steve's Talk]

Our Approach

- Leave the analysis of algebraic attacks against the structure of DH within the **computational model**
- Look for an abstract property that captures DH
- In particular, treat Diffie-Hellman as (ideal) Key Encapsulation Mechanism (KEM)

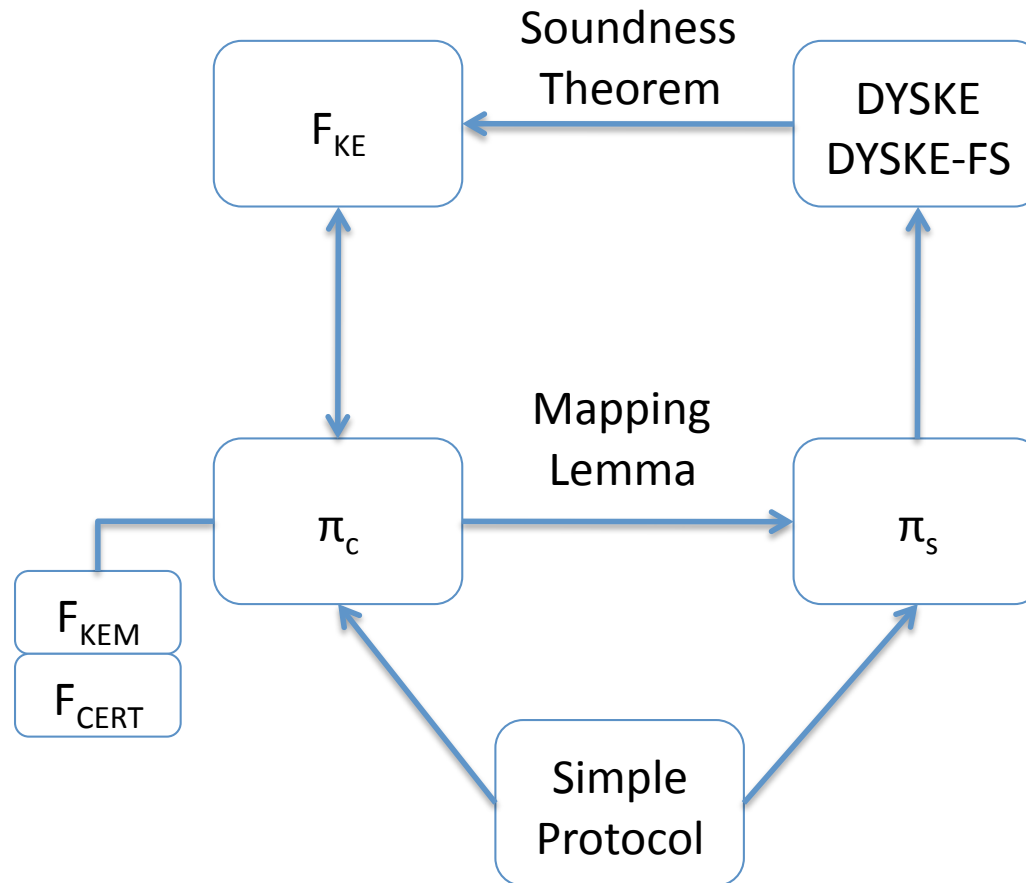
Contributions

- Extend Canetti-Herzog model
 - KEM, Certification, dynamic corruption
- Provide new symbolic criterion
 - key exchange, forward secrecy
- Prove computational soundness for DHKE protocols
- Analyze variants of ISO9738 protocol in ProVerif (e.g. IPsec, SSL)

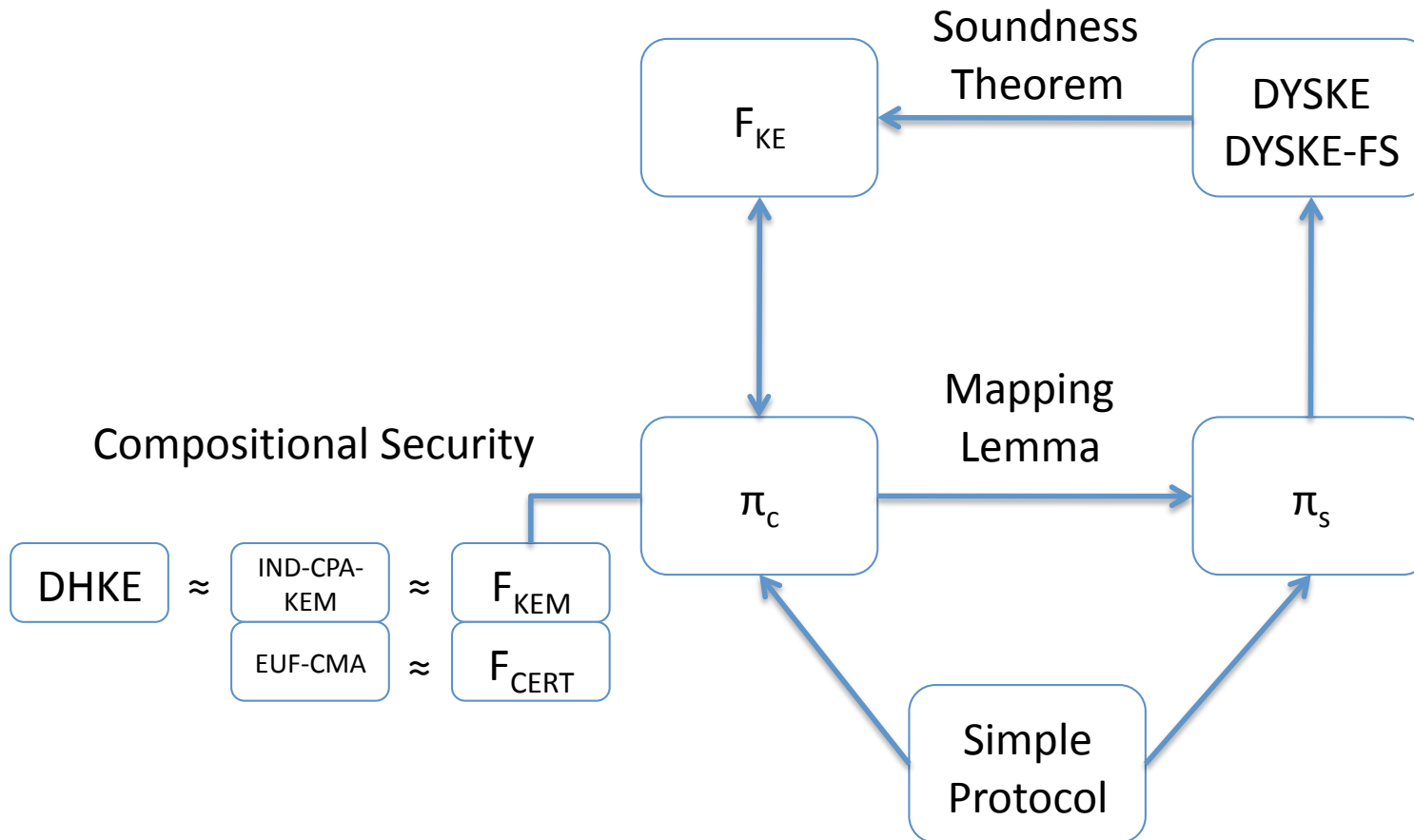
Remainder of the Talk

- Canetti-Herzog model
- Key Encapsulation Mechanism (KEM)
- DHKE securely realizes (ideal) KEM
- Dolev-Yao Criterion for secure Key Exchange
- Forward Secrecy

CH'06 Model



CH'06 Model

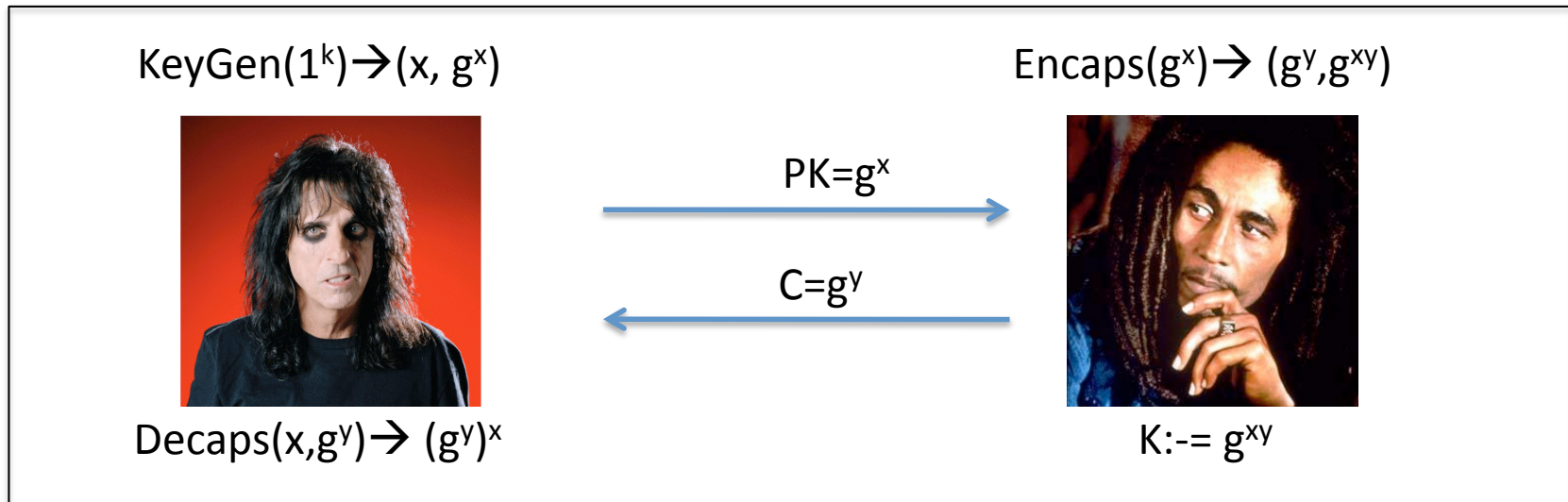


Key Encapsulation Mechanism (KEM)

- A KEM is tuple (KeyGen, Encaps, Decaps)
 - $\text{KeyGen}(1^k) \rightarrow (\text{SK}, \text{PK})$
 - $\text{Encaps}(\text{PK}) \rightarrow (\text{C}, \text{K})$
 - $\text{Decaps}(\text{SK}, \text{C}) \rightarrow \text{K}$
- A KEM is a *one-time encryption* of a randomly chosen key
 - Note: No key cycles !!!

Why is plain-DH a KEM?

- A KEM is tuple (KeyGen, Encaps, Decaps)
 - KeyGen(1^k) \rightarrow (SK, PK) := (x, g^x)
 - Encaps(PK) \rightarrow (C, K) := (g^y, g^{xy})
 - Decaps(SK, C) \rightarrow K := $(g^y)^x$



Protocol π_{DH}

Tools

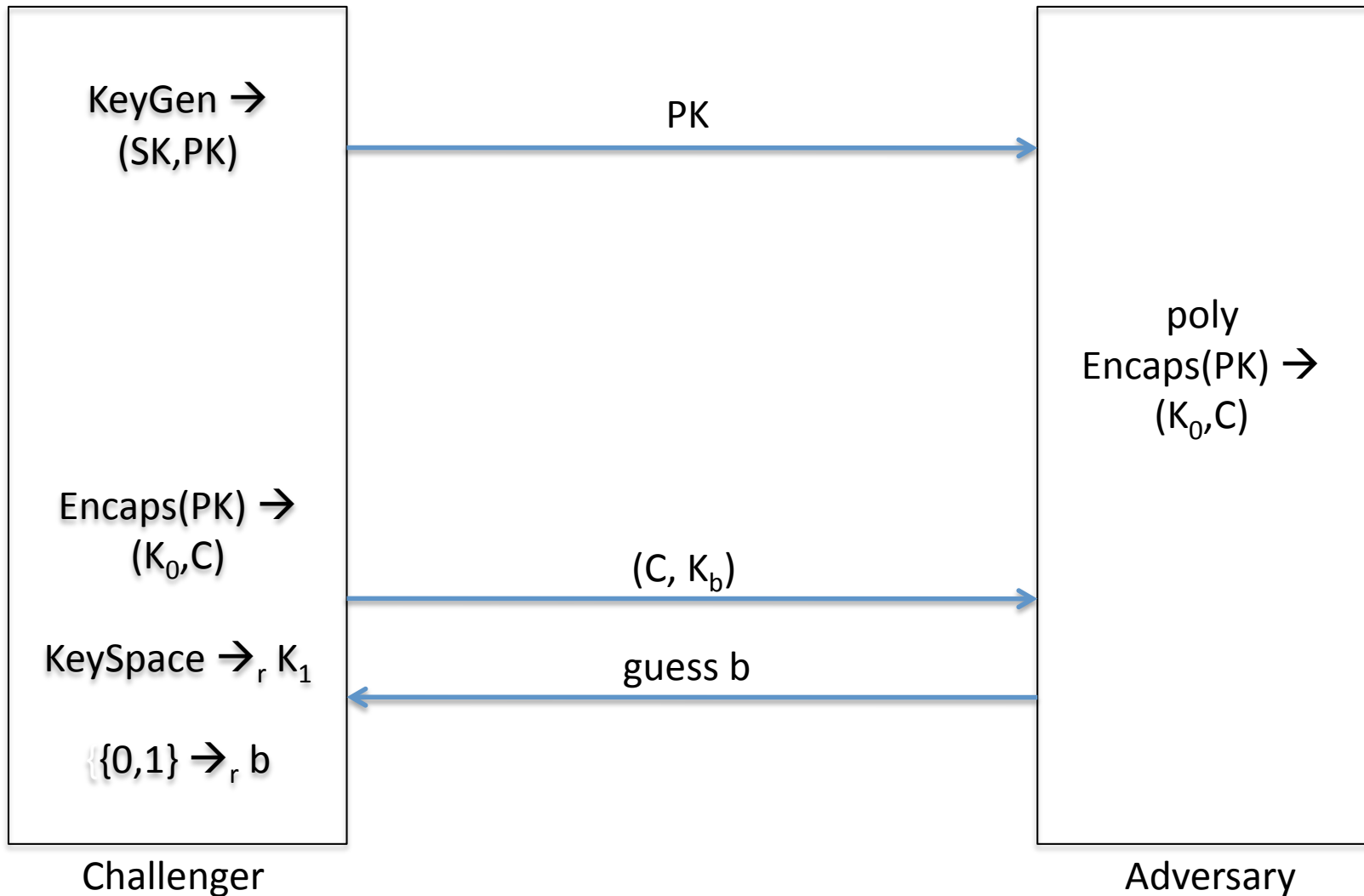
Theorem

π is IND-CPA-KEM secure and no forbidden event, if and only if π UC-realizes F_{KEM}

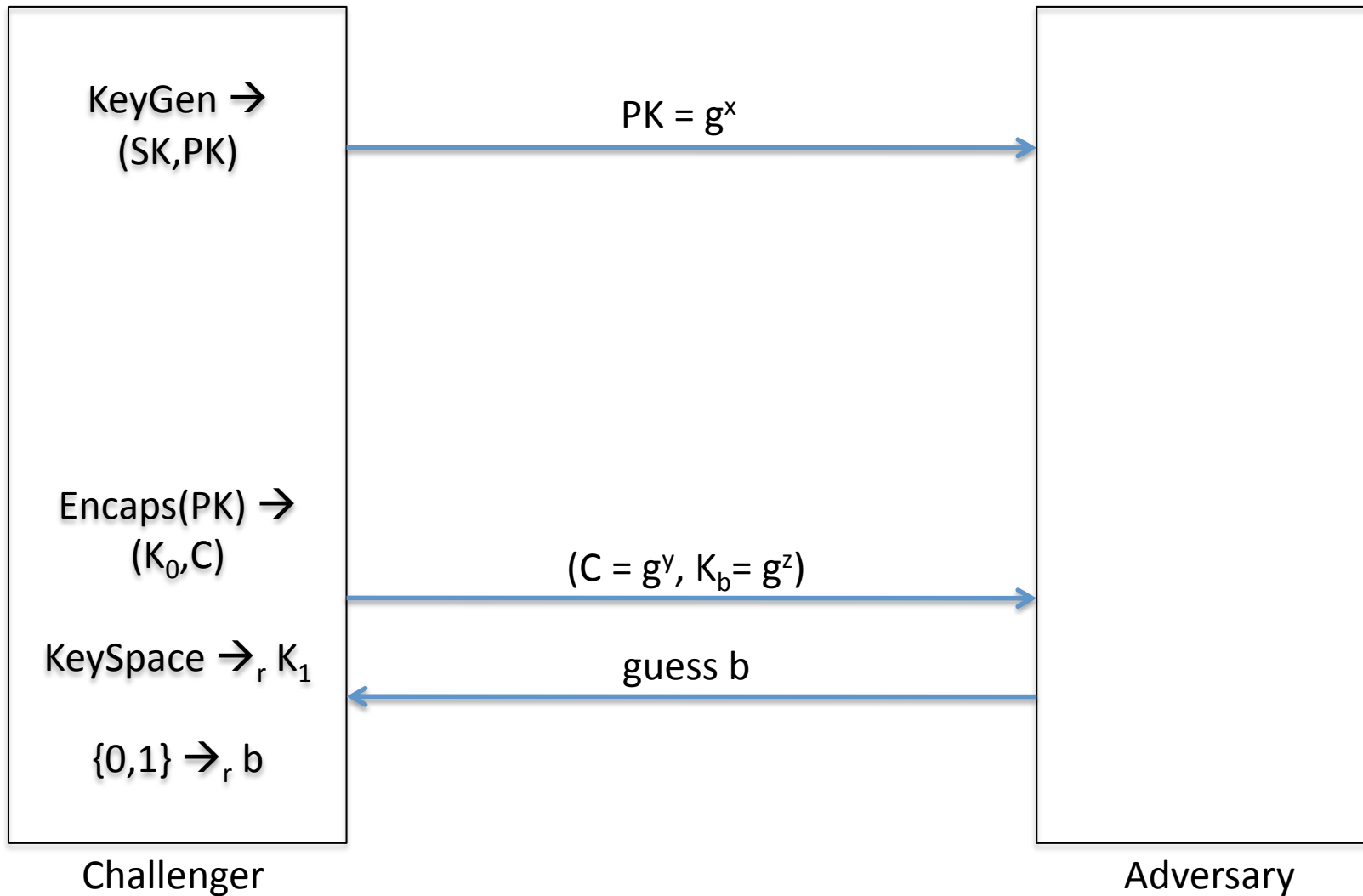
Corollary

Assume the *DDH assumption* holds, then protocol π_{DH} is IND-CPA-KEM secure

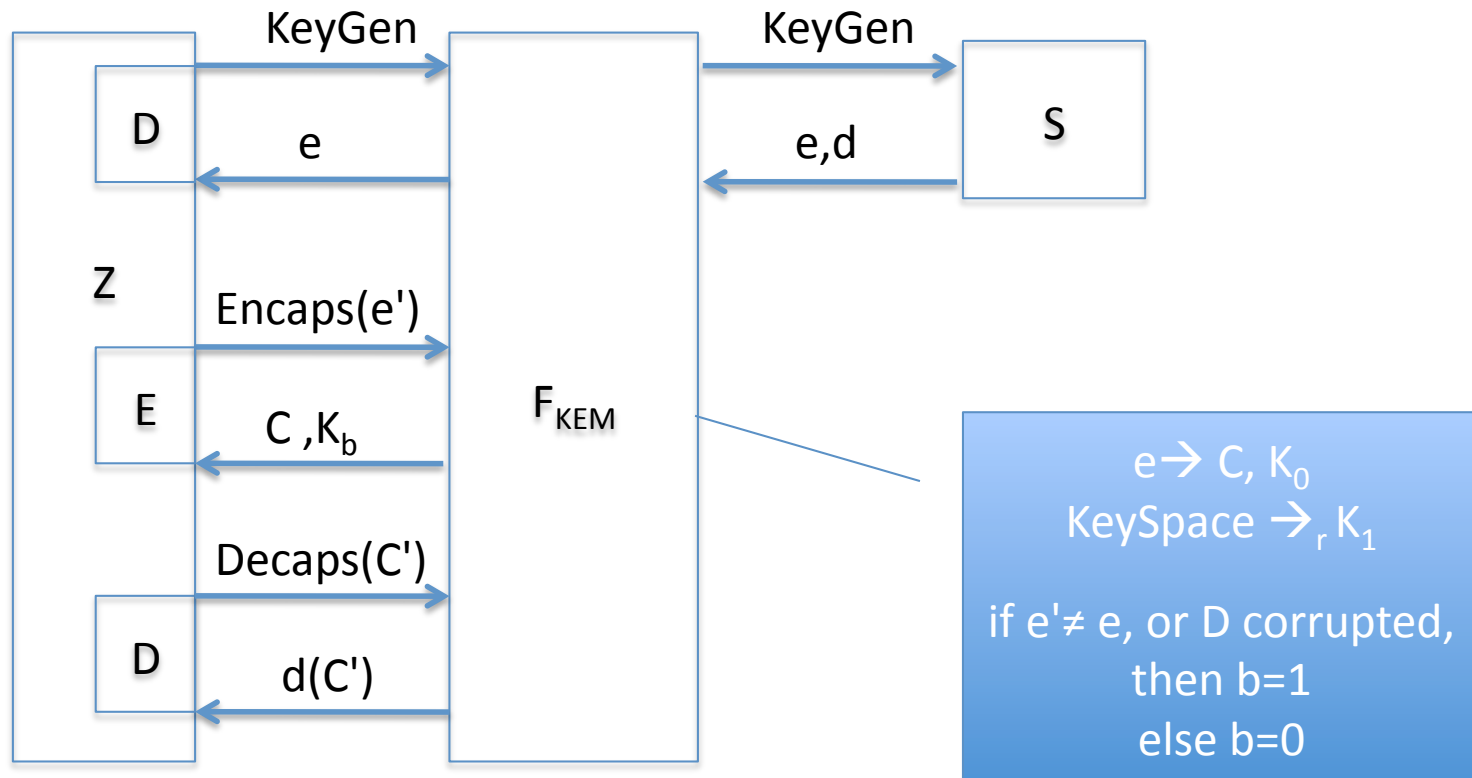
IND-CPA-KEM Security



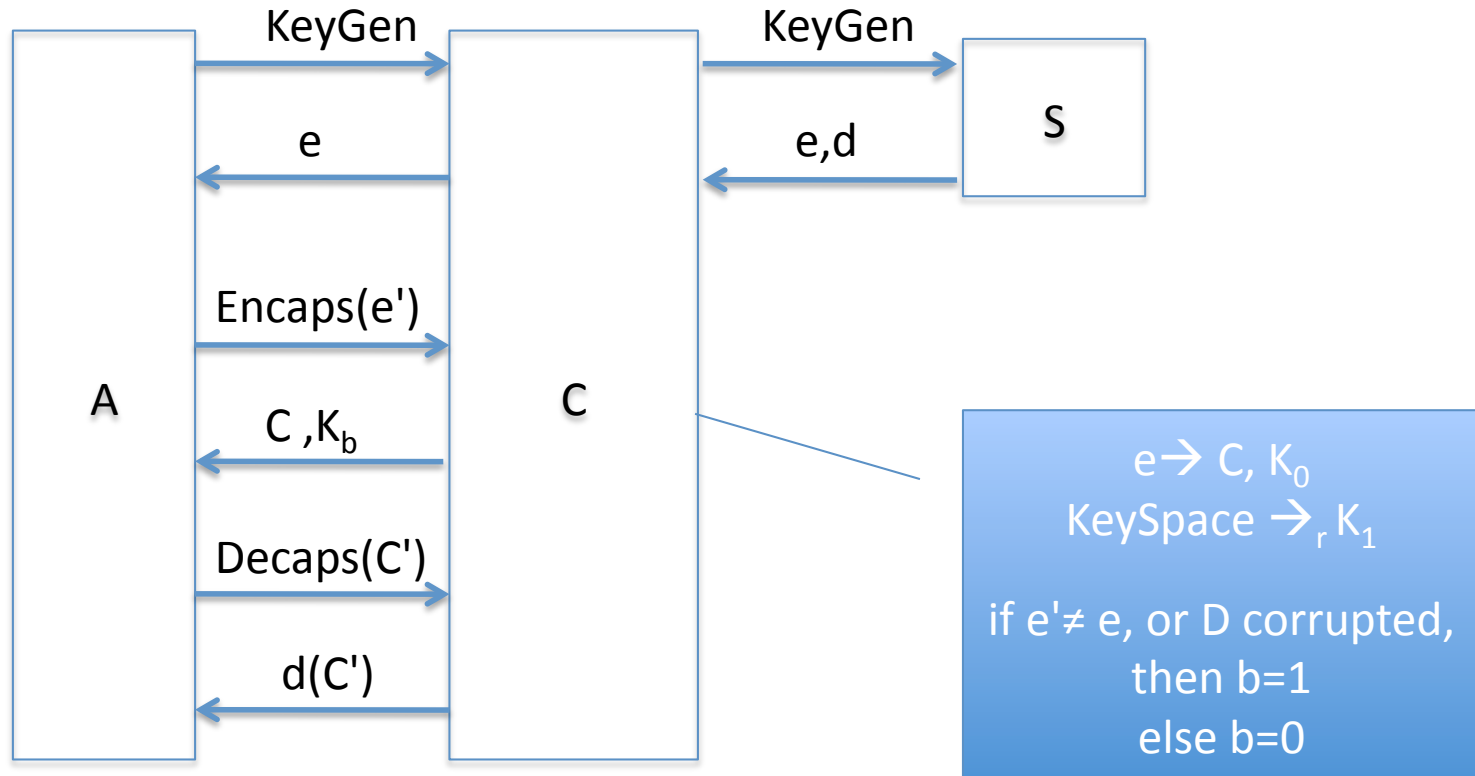
IND-CPA-KEM \rightarrow DDH



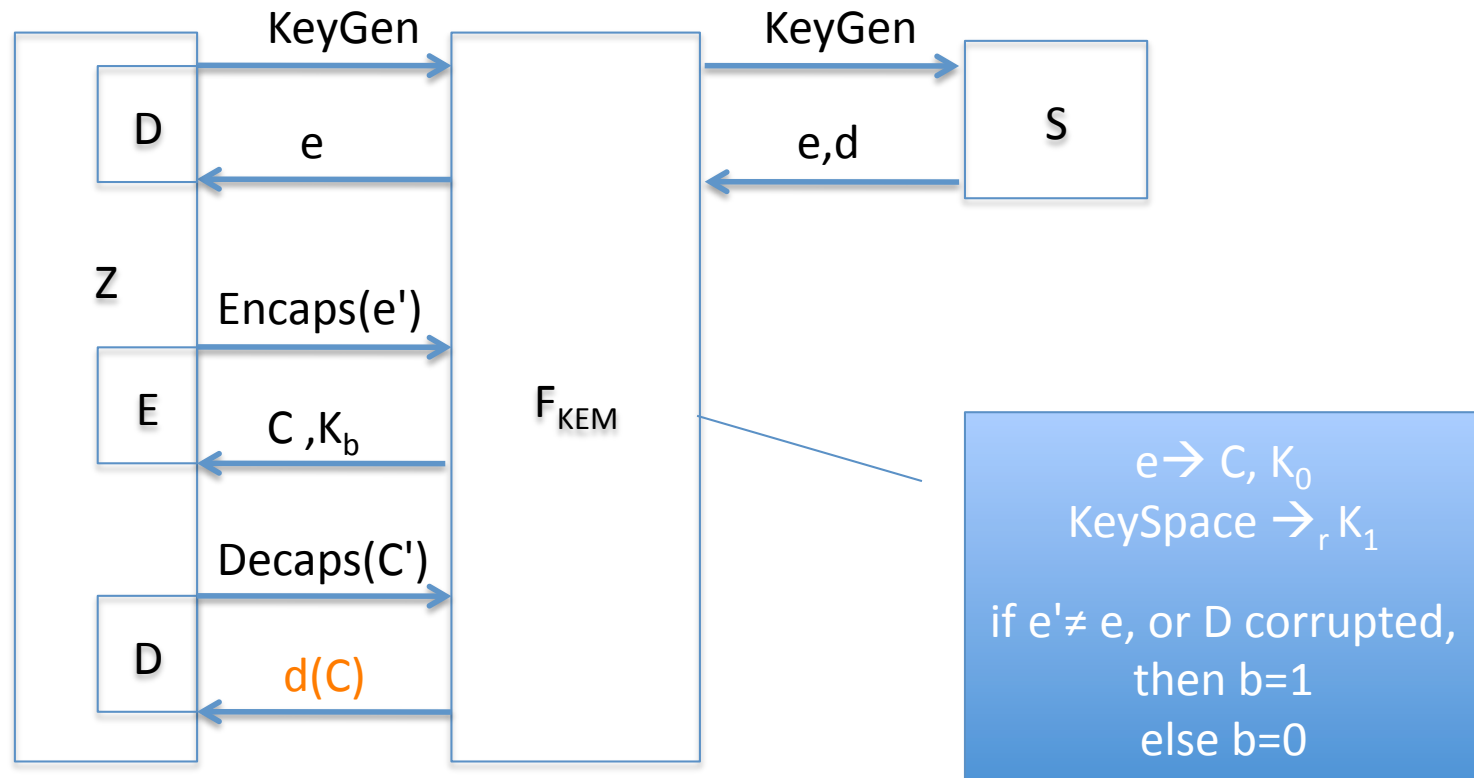
Functionality F_{KEM}



$F_{\text{KEM}} \iff \text{IND-CCA2-KEM}$



$F_{\text{KEM}} \iff \text{IND-CPA-KEM}$



Condition Environment ^[BDHK08]:

F_{KEM} decapses ciphertexts it has seen before
 Otherwise, output **forbidden** query

Remarks

- Add bug to F_{KEM}
 - Functionality outputs **forbidden** query
- Is it meaningful to condition the Environment?
 - Loose universal composability
 - Composable in environments where surrounding protocol protects from forbidden event

DYSKE Criterion

- **Agreement:** For all P_0 and P_1 , in which participant P_0 outputs $\langle \text{establish-key}, P_0, P_1 \rangle$, and participant P_1 outputs $\langle \text{establish-key}, P_1, P_0 \rangle$, if P_0 produces output $\langle \text{key}, m_0 \rangle$ and P_1 produces $\langle \text{key}, m_1 \rangle$, then $m_0 = \langle P_0, P_1, r \rangle$ and $m_1 = \langle P_1, P_0, r \rangle$
- **Real-or-Random Secrecy** For all traces t , $\text{pattern}[t(\text{real})] = \text{pattern}[t(\text{real})]$ after renaming.
- **Encapsulation Test** No message of the form $["\text{forbidden}"]$ exists in the trace

Main Result 1

Theorem (Soundness)

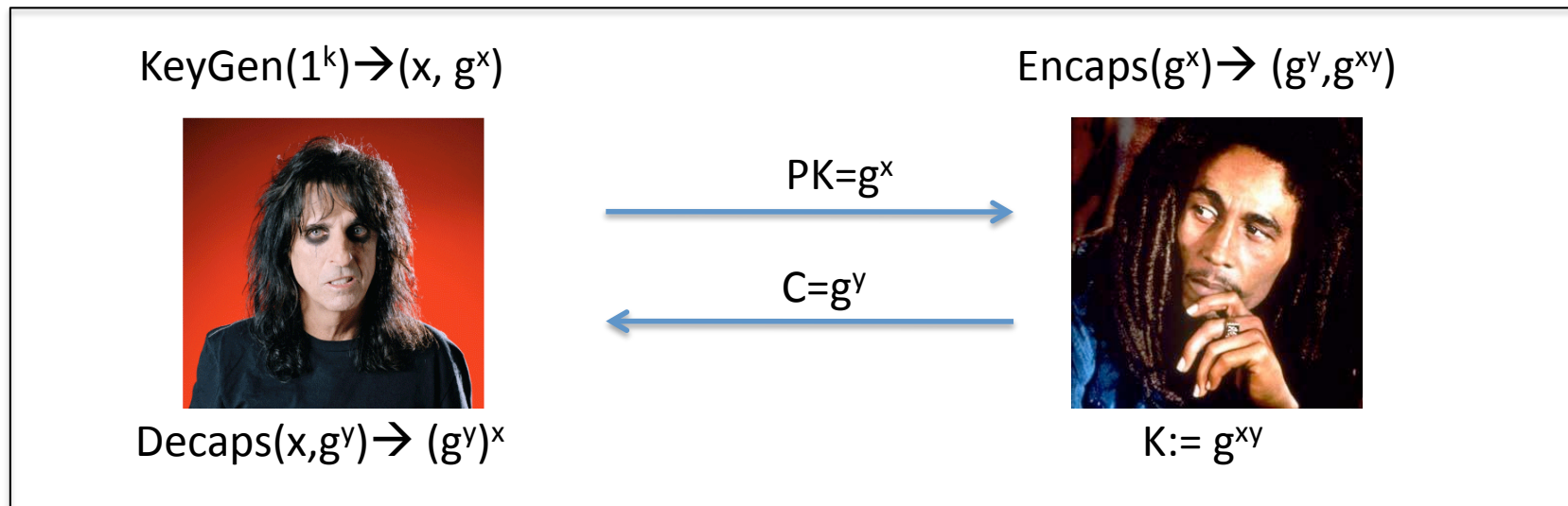
Let π be a simple protocol (that uses KEM and Signatures).
Then π_c realizes F_{KE} with static corruptions, if and only π_s
satisfies DYSKE criterion

(Perfect) Forward Secrecy

- Session key secrecy despite compromise of long-term secrets/past sessions
- Special case: party B terminated and gets compromised, although party A has not output the session key yet
- Commitment problem with F_{KEM} : simulator S for π_{DH} has to come up with **internal state** of compromised party

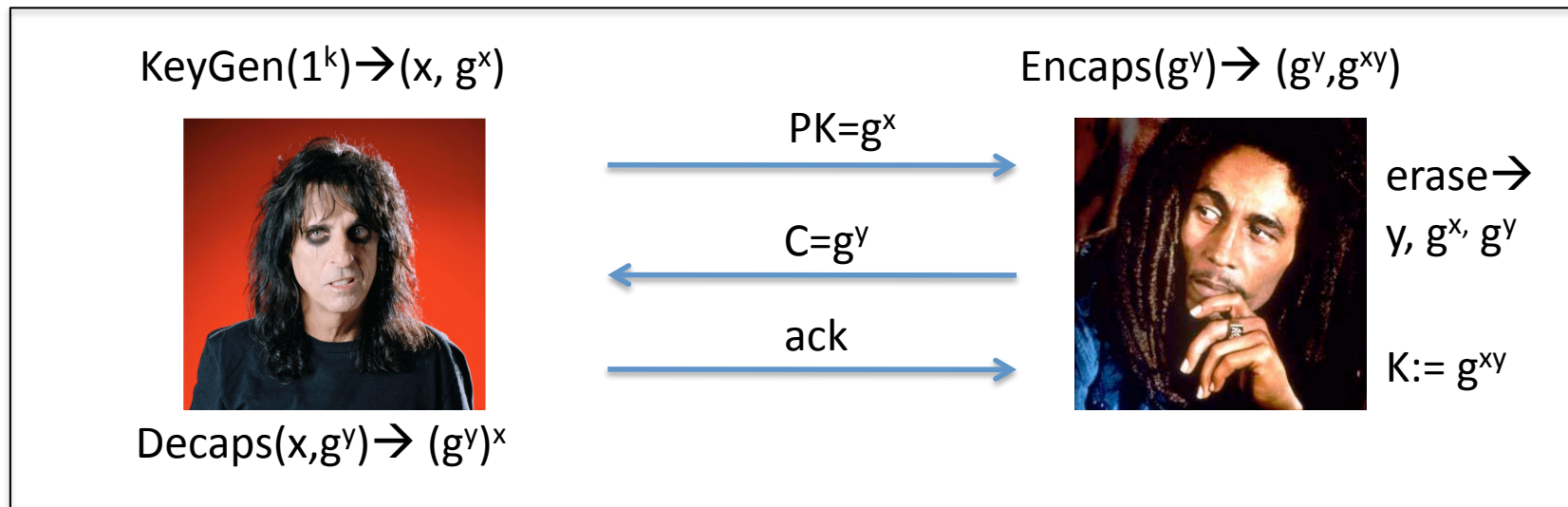
π_{DH} does not UC-realize F_{KEM} under dynamic corruptions

- Adversary corrupts Alice **prior** to delivery of $C = g^y$
 - Real Trace: $g^x, g^y, K = g^{xy}$ and x
 - Ideal Trace: $g^{x'}, g^{y'}, K = g^r$ and x' s.t. $g^{x'y'} = g^r$



Fix the Commitment Problem

- Additional condition for F_{KEM} :
 - Alice must output session key K **prior** to Bob
 - Otherwise, F_{KEM} outputs **early-corrupt**
- Use secure erasure + ack property [CFG96,CK02]



DYSKE-FS

- **Agreement:** For all P_0 and P_1 , in which participant P_0 outputs $\langle \text{establish-key}, P_0, P_1 \rangle$, and participant P_1 outputs $\langle \text{establish-key}, P_1, P_0 \rangle$, if P_0 produces output $\langle \text{key}, m_0 \rangle$ and P_1 produces $\langle \text{key}, m_1 \rangle$, then $m_0 = \langle P_0, P_1, r \rangle$ and $m_1 = \langle P_1, P_0, r \rangle$
- **Real-or-Random Secrecy** For all traces t , $\text{pattern}[t(\text{real})] = \text{pattern}[t(\text{real})]$ after renaming
- **Encapsulation Test 1** No message of the form $["\text{forbidden}"]$ exists in the trace
- **Encapsulation Test 2** No message of the form $["\text{early-corrupt}"]$ exists in the trace

Main Result 2

Theorem (Soundness)

Let π be a simple protocol (that uses KEM and Signatures).
Then π_c realizes F_{KE} with dynamic corruptions, if and only π_s satisfies DYSKE-FS criterion (in the symbolic model with dynamic corruptions)

Summary

- Extended Canetti-Herzog model
 - Diffie-Hellman key exchange
 - Certification
- Presented new security criterion
 - universal composable key exchange
 - forward security
- Enriched the picture of computationally sound analysis of key exchange protocols

Open Problems

- Generalize Canetti-Herzog [C-Gajek15]
 - security for any cryptographic task
 - composition in symbolic model
- Analyze "sophisticated" tasks [C-Gajek15+x]
 - secure channels, ZK, MPC, ...
 - browser-based protocols, file-systems,
- Implement Theory [C-Gajek15+y]
 - Ideal functionality specification
 - Automated construction of simulator