Generic Security Solutions for Group Key Exchange

Mark Manulis

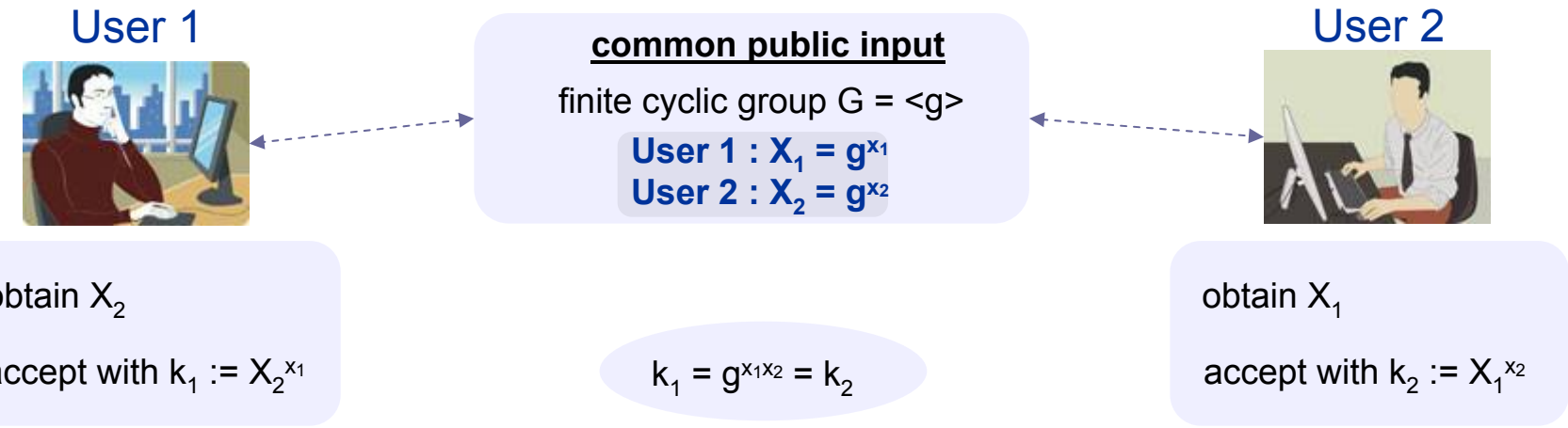
Fakultät für Elektro- und Informationstechnik

Ruhr Universität Bochum

Juni 26, 2007

„Genuine“ Diffie-Hellman Key Exchange[DH76]

- 2-party key exchange protocol proposed by Diffie and Hellman in 1976
- foundational for many group key exchange protocols[ITW82,SSDW88,BD94,…]
- computations are performed in the *finite cyclic* group G
  - g is the generator of G
  - *Discrete Logarithm Problem* (given g^x find x) is intractable in G



„Referenced“ Diffie-Hellman Key Exchange

- users choose own secret exponents during the protocol execution

User 1

common public input

finite cyclic group G = <g>

User 2

choose random x_1

$X_1 := g^{x_1}$

accept with $k_1 := (X_2)^{x_1}$

X_1 →

← X_2

← X_2

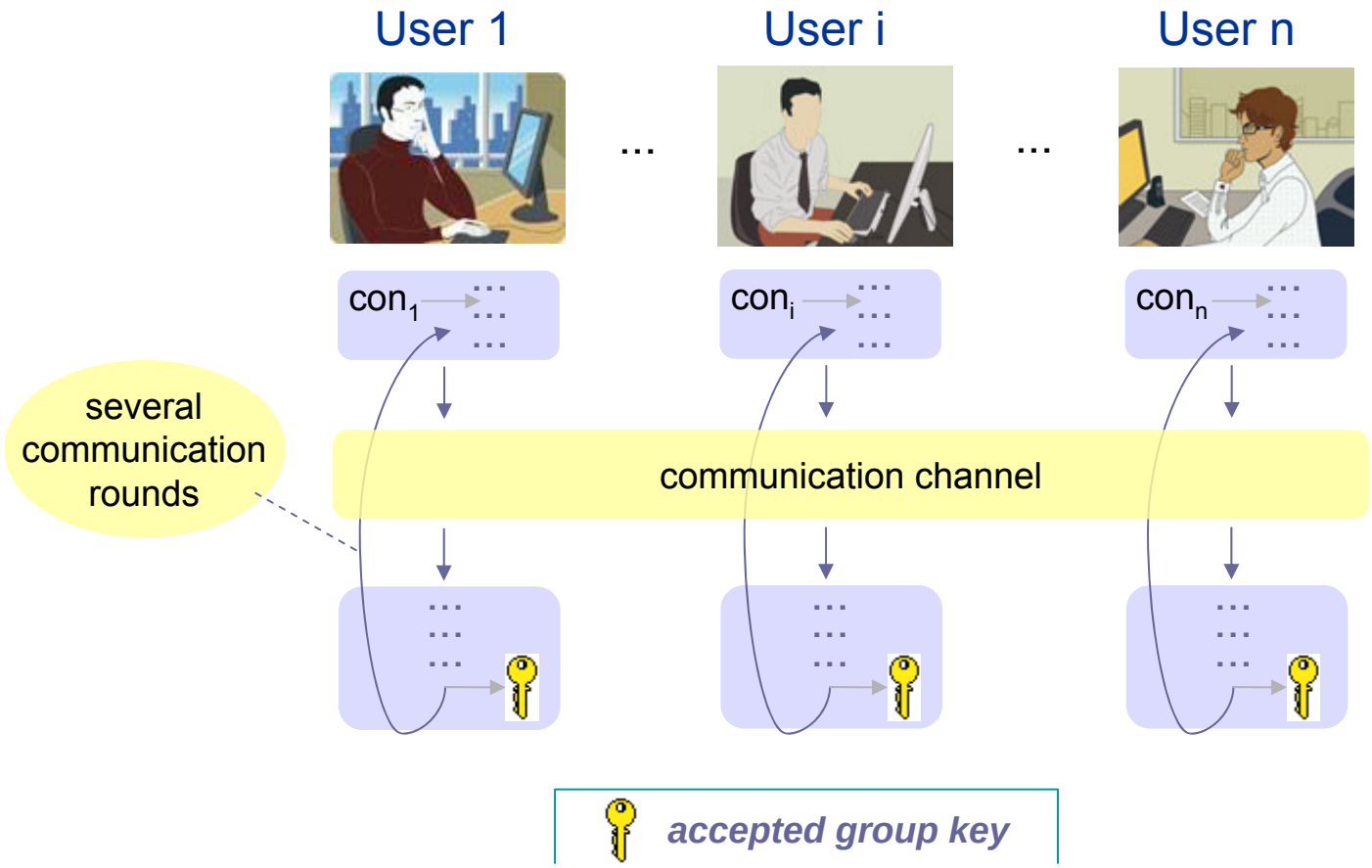
X_1 →

choose random x_2

$X_2 := g^{x_2}$

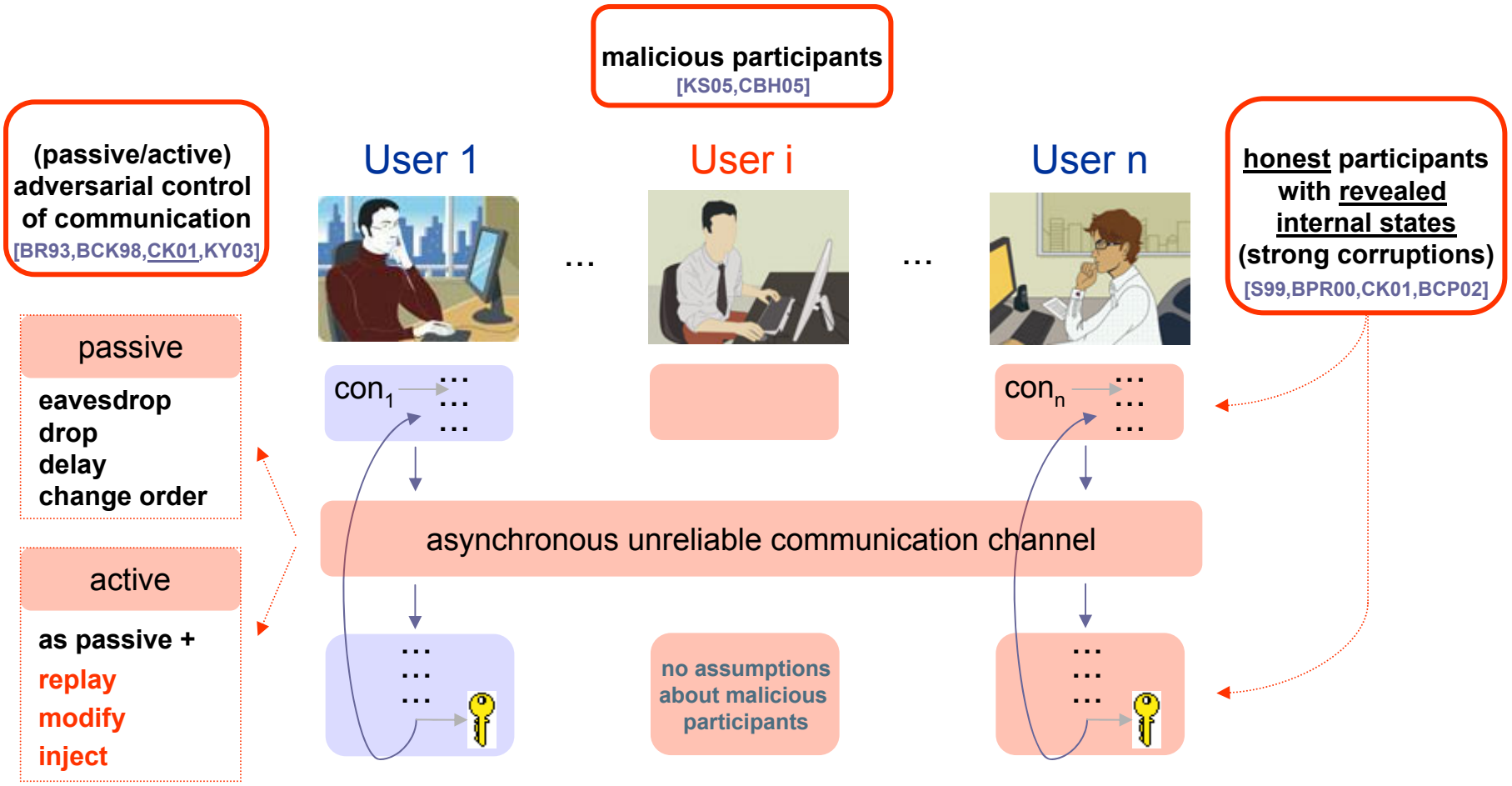
accept with $k_2 := (X_1)^{x_2}$

Group Key Exchange (GKE)

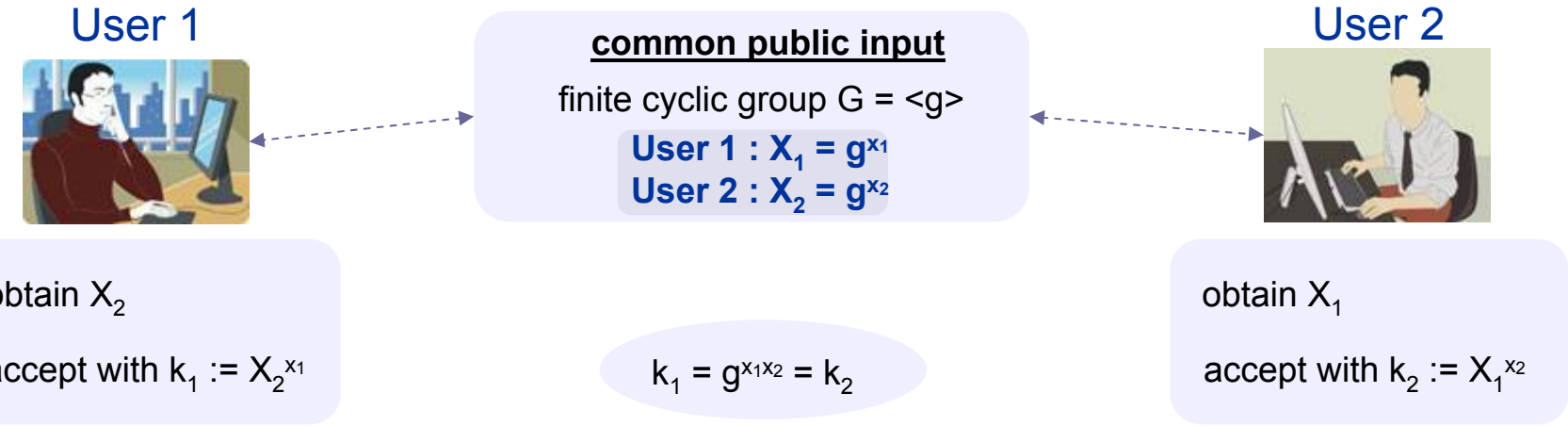


con_i secret contribution of User i

Security Threats in GKE

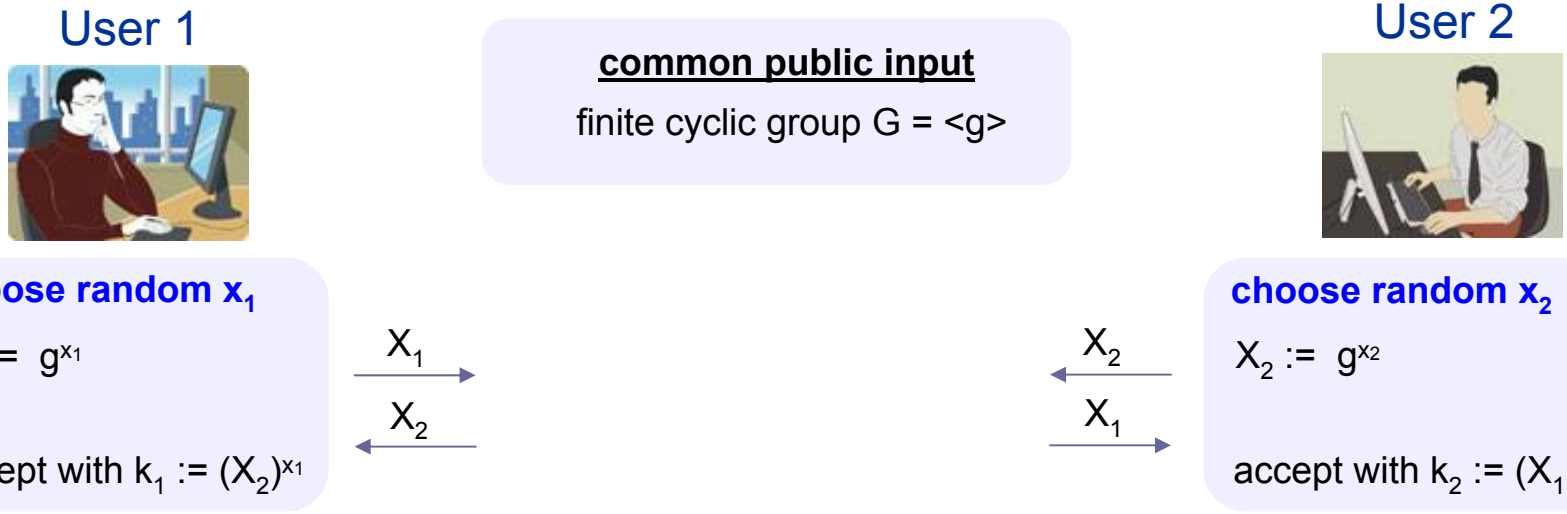


Security Observations for „Genuine“ DH-KE



- every new session results in the same key
  - (–) no key secrecy if other session keys are exposed (known-key security)[B94]
- long-term keys (x_1,x_2) used directly to compute the key
  - (–) no key secrecy if (x_1,x_2) are exposed later (weak forward secrecy)[G89]
- long-term keys are linked to the users‘ identities
  - (+) adversary cannot act on behalf of the users (impersonation resilience)[BD94]

Security Observations for „Referenced“ DH-KE



- session keys are independent in different sessions
  - (+) known-key security is provided
- no long-term keys are used
  - (+) weak forward secrecy is provided, *but*
  - (–) impersonation attacks become possible
- ephemeral secrets (x_1,x_2) are used to compute the key
  - (–) no key secrecy if (x_1,x_2) are exposed later (strong forward secrecy) [BPR00,CK01]

Achieving Strong Forward Secrecy

- Idea: *erase ephemeral secrets* prior to acceptance, e.g., *secure erasure*[CFIJ99]

User 1

common public input

finite cyclic group G = <g>

User 2

choose random x_1

$X_1 := g^{x_1}$

$k_1 := (X_2)^{x_1}$

erase x_1

accept with k_1

X_1 →

← X_2

X_2 ←

→ X_1

choose random x_2

$X_2 := g^{x_2}$

$k_2 := (X_1)^{x_2}$

erase x_2

accept with k_2

- ephemeral secrets used to compute the key are erased
  - (+) strong forward secrecy

- no long-term keys are used
  - (+) weak forward secrecy is provided, *but*
  - (–) impersonation attacks still possible

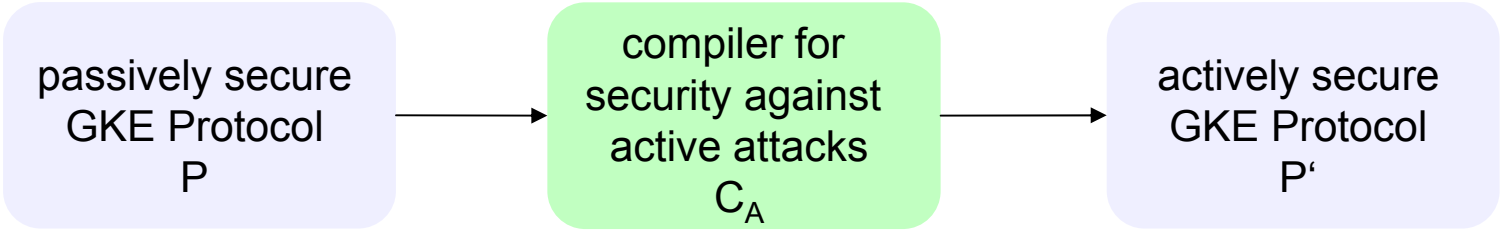
Generic Solution against Active Attacks

Passive Attacks[CK01]

eavesdrop, drop, delay, change order

Active Attacks

replay, modify, inject



Building Blocks

- *digital signature scheme* (Gen, Sign, Verify)
  - every User i is in possession of a long-term key pair $(sk_i,pk_i) \leftarrow$ Gen
  - every pk_i is publicly known and linked to User i
  - provides *existential unforgeability*

Security Compiler C_A

User 1

(pk_1, sk_1)

common public input

User 1 : pk_1
User 2 : pk_2

pid_1 = **User 1**|**User 2** = pid_2

(pk_2, sk_2)

User 2

choose random r_1

$sid_1 = r_1|r_2$

r_1 →

← r_1

computation of the unique session id

r_2 →

← r_2

choose random r_2

$sid_2 = r_1|r_2$

P

m →

σ_1 = Sign(**sk_1**, m|sid_1|pid_1)

$m|\sigma_1$ →

$m|\sigma_2$ ←

σ_1 = Sign(**sk_2**, m|sid_2|pid_2)

← m

P

← m

Verify(**pk_2**, m|sid_1|pid_1, **σ_2**)

Verify(**pk_1**, m|sid_2|pid_2, **σ_1**)

m →

k_1

k_2

accept with k_1

accept with k_2

r_i **random nonce (number used once)** pid_i **partner id**

C_A-compiled „Referenced“ DH-KE

User 1

(pk_1, sk_1)

common public input

User 1 : pk_1
User 2 : pk_2

(pk_2, sk_2)

User 2

$sid_1 = r_1|r_2$

computation of the unique session id

$sid_2 = r_1|r_2$

choose random x_1

$X_1 := g^{x_1}$

$k_1 := (X_2)^{x_1}$

erase x_1

$X_1|\sigma_1$ →

← $X_2|\sigma_2$

asynchronous unreliable communication channel

$X_2|\sigma_2$ →

← $X_1|\sigma_1$

choose random x_2

$X_2 := g^{x_2}$

$k_2 := (X_1)^{x_2}$

erase x_2

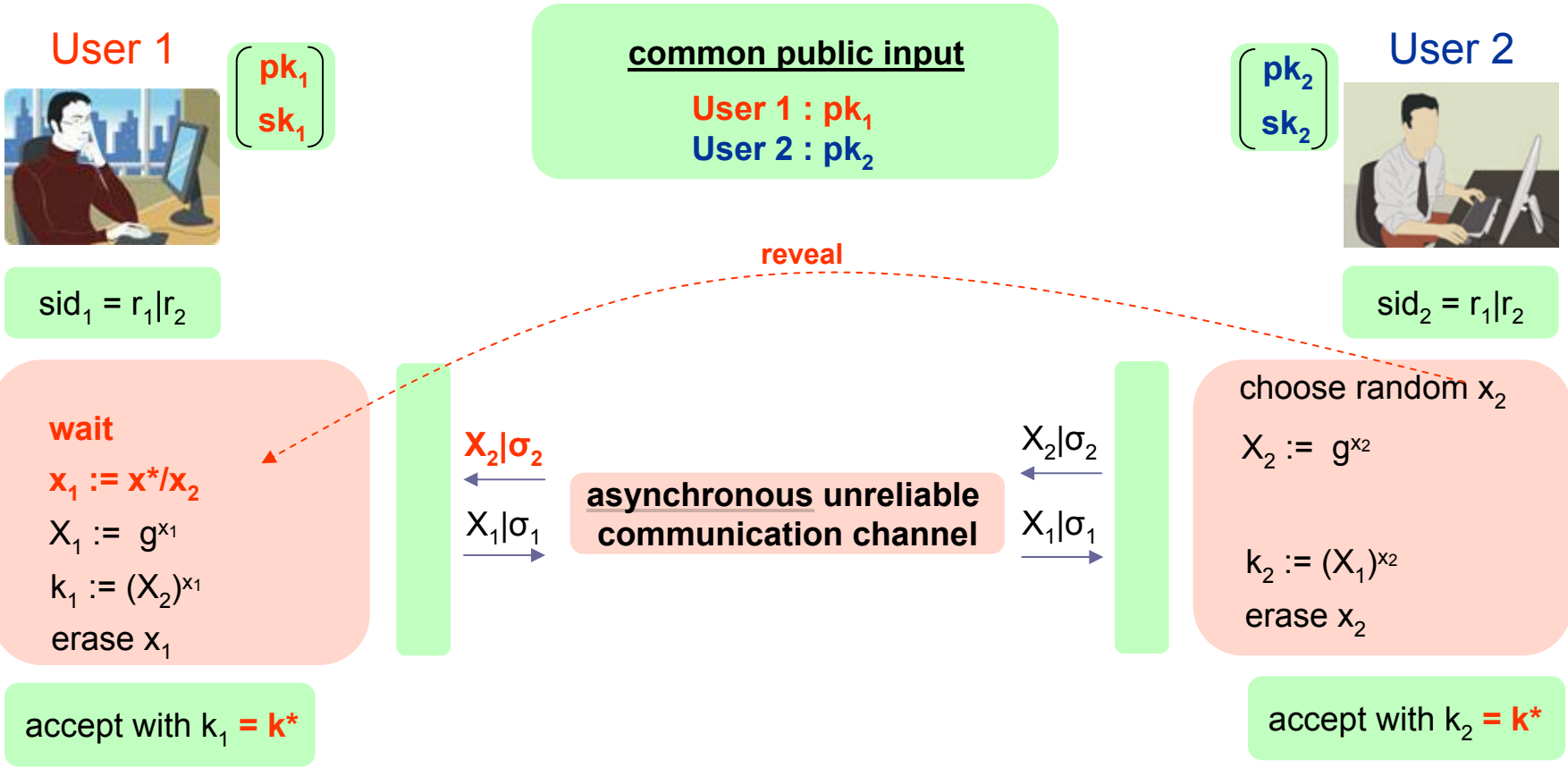
accept with k_1

accept with k_2

- Recall: malicious participants may deviate from the protocol specification and internal states of honest participants may be revealed
  - malicious user can *exclude contribution* of the honest user upon computing k (key control[MWW98], contributiveness[AST98], key replication[K05])

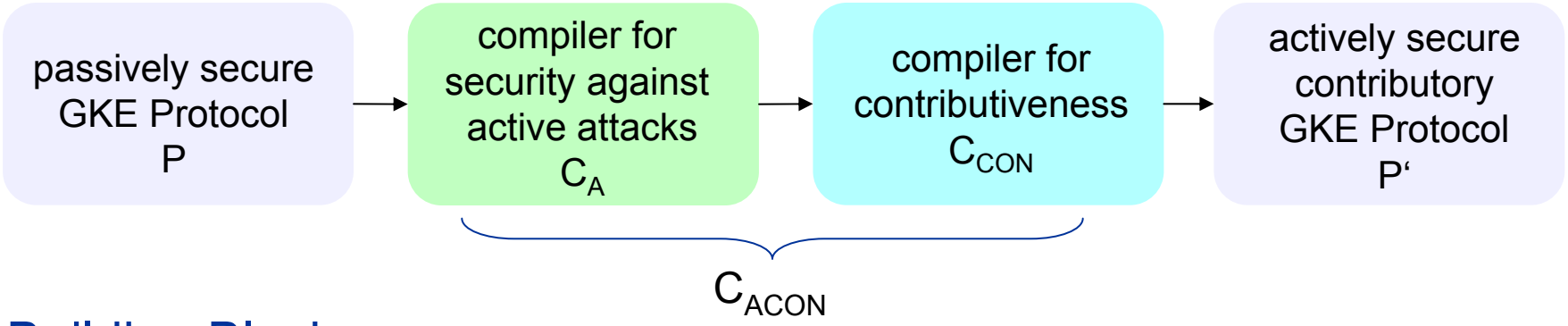
Attack against Contributiveness

- malicious User 1 wishes that User 2 accepts $k^* = g^{x^*}$ for *some chosen* x^*



- malicious User 1 succeeds for ***any*** choice of x_2 in ***any*** protocol session

Generic Solution for Contributiveness



Building Blocks

- *collision-resistant pseudo-random function* f(s, v)
  - s – uniformly chosen secret seed, v – (public) input value
  - *collision-resistance*

    for all s ≠ s‘ holds f(s,v) ≠ f(s‘,v)
  - *pseudo-randomness*

    outputs f(s,·) are indistinguishable from randomly chosen values
- *one-way permutation* π
  - *one-wayness*

    given π(x) it is infeasible to find x

Security Compiler C_{ACON}

User 1

(pk_1, sk_1)

common public input

User 1 : pk_1
User 2 : pk_2

v

User 2

(pk_2, sk_2)

$sid_1 = r_1|r_2$

computation of the unique session id

$sid_2 = r_1|r_2$

P | Sign Verify

Sign Verify | P

k_1

k_2

$\rho_0 := f(k_1, v)$

$\rho_1 := f(\rho_0 \oplus \pi(r_1), v)$

$\rho_2 := f(\rho_1 \oplus \pi(r_2), v)$

$K_1 := \rho_2$

erase $k_1, \rho_0, \rho_1, \rho_2$

iterative embedding of r_i
no further communication is needed

$\rho_0 := f(k_2, v)$

$\rho_1 := f(\rho_0 \oplus \pi(r_1), v)$

$\rho_2 := f(\rho_1 \oplus \pi(r_2), v)$

$K_2 := \rho_2$

erase $k_2, \rho_0, \rho_1, \rho_2$

accept with K_1

accept with K_2

Presented Dissertation Results

- Compiler for Security against Active Attacks C_A
  - generic solution against replication, modification, and injection
  - under consideration of strong corruptions

- C_A with Add-on Compiler for Contributiveness C_{ACON}
  - generic solution against replication, modification, and injection
  - generic solution against attacks on contributiveness
  - under consideration of strong corruptions

Further Dissertation Results

- „Provable Security“ Issues
  - analysis and comparison of
    - 12 security models and 3 variations
    - 12 provably secure GKE protocols
  - enhanced security model with extended definitions
  - under consideration of *dynamic* GKE protocols
- Generic Security Solutions (in addition to C_A and C_{ACON})
  - compiler for *mutual authentication and key confirmation* (C_{MA})
  - 4 combinations of C_A, C_{CON}, and C_{MA}
  - security proofs wrt. the proposed security model
- Constant-Round GKE Protocol TDH1
  - static and dynamic versions
  - security proofs wrt. the proposed security model

Thank You

Bibliography

[AST98] G. Ateniese, M. Steiner, and G. Tsudik. *Authenticated Group Key Agreement and Friends.* 5th ACM Conference on Computer and Communications Security (CCS'98), pp. 17–26, 1998.

[BCK98] M. Bellare, R. Canetti, and H. Krawczyk. *A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols (Extended Abstract).* 13th Annual ACM Symposium on the Theory of Computing (STOC'98), pp. 419–428, 1998.

[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway. *Authenticated Key Exchange Secure Against Dictionary Attacks.* In Advances in Cryptology –EUROCRYPT'00, LNCS vol. 1807, pp. 139–155, 2000.

[BR93] M. Bellare and P. Rogaway. *Entity Authentication and Key Distribution.* In Advances in Cryptology – CRYPTO'93, LNCS vol. 773, pp. 232–249, 1993

[BCP02] E. Bresson, O. Chevassut, and D. Pointcheval. *Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions.* In Advances in Cryptology – EUROCRYPT'02, LNCS vol. 2332, pp. 321–336, 2002.

[B94] M. Burmester. *On the Risk of Opening Distributed Keys.* In Advances in Cryptology – CRYPTO'94, LNCS vol. 839, pp. 308–317, 1994.

[BD94] M. Burmester and Y. Desmedt. *A Secure and Efficient Conference Key Distribution System.* In Advances in Cryptology – EUROCRYPT'94, LNCS vol. 950, pp. 275–286, 1994.

[CK01] R. Canetti and H. Krawczyk. *Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels.* In Advances in Cryptology - EUROCRYPT'01, LNCS vol. 2045, pp. 453–474, 2001.

[CBH05] K.-K. R. Choo, C. Boyd, and Y. Hitchcock. *Examining Indistinguishability-Based Proof Models for Key Establishment Protocols.* In Advances in Cryptology – ASIACRYPT'05, LNCS vol. 3788, pp. 585–604, 2005.

[CFIJ99] G. D. Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. *How to Forget a Secret.* 16th Annual Symposium on Theoretical Aspects of Computer Science (STACS'99), LNCS vol. 1563, pp. 500–509, 1999.

[G89] C. G. Günther. *An Identity-Based Key-Exchange Protocol.* In Advances in Cryptology – EUROCRYPT'89, LNCS vol. 434, pp. 29–37, 1990.

[ITW82] I. Ingemarsson, D. T. Tang, and C. K. Wong. *A conference key distribution system.* IEEE Transactions on Information Theory, 28(5):714-719, 1982.

[KS05] J. Katz and J. S. Shin. *Modeling Insider Attacks on Group Key-Exchange Protocols.* 12th ACM Conference on Computer and Communications Security (CCS'05), pp. 180–189, 2005.

[KY03] J. Katz and M. Yung. *Scalable Protocols for Authenticated Group Key Exchange.* In Advances in Cryptology - CRYPTO'03, LNCS vol. 2729, pp. 110–125, 2003.

[K05] H. Krawczyk. HMQV: A High-Performance Secure Diffie-Hellman Protocol. In Advances in Cryptology – CRYPTO'05, LNCS vol. 3621, pp. 546–566, 2005.

[MWW98] C. J. Mitchell, M. Ward, and P. Wilson. *Key Control in Key Agreement Protocols.* Electronic Letters, 34(10):980–981, 1998.

[S99] V. Shoup. *On Formal Models for Secure Key Exchange (Version 4).* Technical Report RZ 3120, IBM Research, 1999.

[SSDW88] D. G. Steer, L. Strawczynski, W. Diffie, and M. J. Wiener. *A Secure Audio Teleconference System.* In Advances in Cryptology – CRYPTO'88, LNCS vol. 403, pp. 520–528, 1990.