# Sender-Binding Key Encapsulation

Laurin Benz[1,2] **Wasilij Beskorovajnov[3]** Sarai Eilebrecht[3] Jörn Müller-Quade[1,2,3] Astrid Ottenhues[1,2] Rebecca Schwerdt[1,2]

[1]Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
[2]KASTEL Security Research Labs, Karlsruhe, Germany
*{laurin.benz, mueller-quade, ottenhues, schwerdt}@kit.edu*

[3]FZI Research Center for Information Technology, Karlsruhe, Germany
*{beskorovajnov, eilebrecht}@fzi.de*

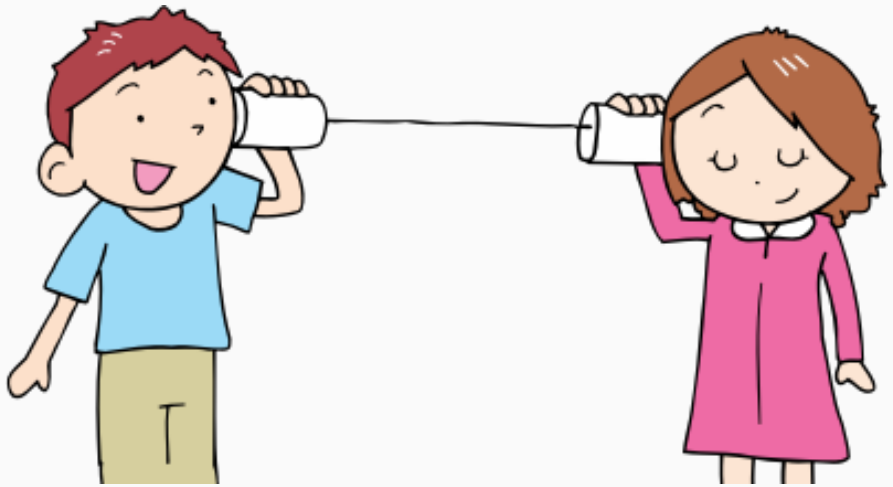
# Preliminaries

- Universal Composability (UC) Framework [3]
- Notions of
  - weak CCA for Tag-based encryption (TBE) or (tag-based) Key encapsulation mechanism (KEM)
  - IND-OT and (R)CCA Data encapsulation mechanism (DEM)
- Hybrid PKE – the KEM/DEM Paradigm, e.g. [7]

# Motivation

# Motivation

- Only CCA2 secure PKE is not enough
  - A Relay-Attack is still possible
  - Authenticated channels are a requirement
- What is an authenticated channel? $\rightarrow$ e.g. a secure signature scheme combined with a secure certification authority



# Motivation

CCA2 security is unncessarily strong ([4, 2, 11])

→ The non-malleability of information passing through an authenticated channel **overlaps** with the non-malleability of the employed IND-CCA2$_{\text{PKE}}$ secure PKE.

# Motivation

This motivation was adressed recently in [2] by showing that a PKE does not to need to be stronger than **sender-binding CPA**.

# Motivation

What about hybrid encryption?

# Related Work

# Related Work on the KEM/DEM Paradigm

Relaxations considering only the DEM

- Shoup [13] showed: IND-CCA2$_{\text{KEM}}$ + IND-CCA2$_{\text{DEM}}$ yields an IND-CCA2$_{\text{PKE}}$ secure PKE as a result.
- First relaxation in [6] to a one-time-IND-CCA2$_{\text{DEM}}$ (sometimes called IND-OTCCA [7]).
- One main finding of Herranz, Hofheinz and Kiltz in [7] was that CCA2 security could so far **only** be reached via a CCA2 secure KEM in conjunction with IND-OTCCA DEM.
- Abe et al. [1] showed IND-CCA2$_{\text{tag-KEM}}$ KEM + IND-OT$_{\text{DEM}}$ DEM yields an IND-CCA2$_{\text{PKE}}$ secure PKE as a result. (This work subsumes the Kurosawa-Desmedt-KEM + DEM from [10])

# Related Work on the KEM/DEM Paradigm

Relaxations considering only the KEM

- Constrained CCA from Hofheinz and Kiltz [8]
- Bounded CCA from Cramer et al. [5]
- Detectable CCA from from Hohenberger et al. [9]
- Replayble CCA from Canetti et al. [4]

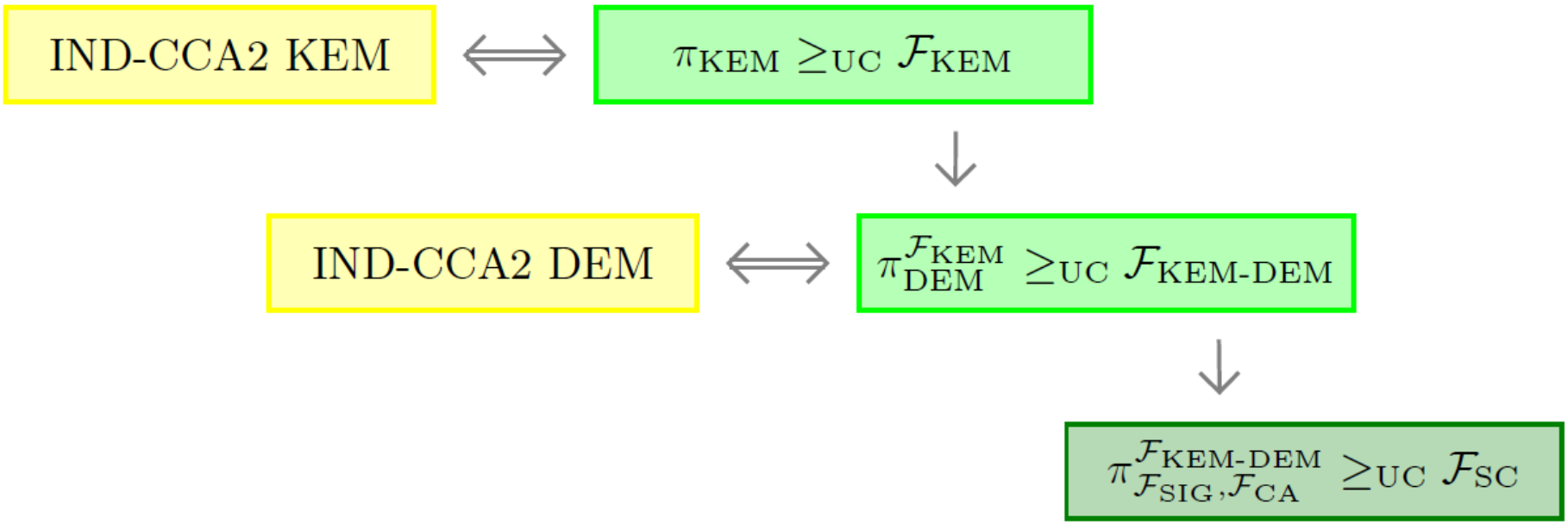
# Related Work's Main Motivation

**A CCA2 secure hybrid PKE $\neq$ Our Motivation**

Moreover, these works consider only the "Single Message Transfer" scenario (e.g., secure e-mail communication)

# Related Work on KEMs and Secure Channels in Universal composability (UC)

Session communication scenario from KEMs by Nagao, Manabe and Okamoto [12] (e.g., SSL, IPSec, SSH)




$\rightarrow$ Is the $\text{CCA2}_{\text{KEM}}$ security necessary?

# Contribution

# Contribution

We introduce two formal notions

- Sender-binding Key encapsulation mechanism (SB-KEM)

  $\mathit{gen} : 1^\lambda \mapsto (sk, pk), \quad \mathit{enc} : (pk, S) \mapsto (K, C), \quad \mathit{dec} : (sk, S, C) \mapsto K$

- Indistinguishability under Sender-binding chosen plaintext attack (IND-SB-CPA) for SB-KEMs

# Single Message Scenario

$$\text{SB-CPA KEM} + \text{OT DEM} \Rightarrow \text{SB-CPA SBE}$$

From [2] we may conclude that this encryption realizes a secure channel in a $F_{AUTH}$ hybrid model.

# Session Communication Scenario

We generalize and relax the results from Nagao, Manabe and Okamoto [12].

$$\pi_{\mathrm{MSC}}^{\mathcal{F}_{\mathrm{AUTH}}} \geq_{\mathrm{UC}} \mathcal{F}_{\mathrm{MSC}}$$

# Intuition of IND-SB-CPA$_{\text{SB-KEM}}$

- IND-SB-CPA$_{\text{SB-KEM}}$ requires
  - **non-malleability of the sender identity** $\rightarrow$ decaps oracle $\mathcal{O}_{\text{SB-CPA}}$
  - **semantic security of the message** $\rightarrow$ indistinguishability experiment
- The authenticated channel protects the rest

# Definition of IND-SB-CPA$_{\text{SB-KEM}}$

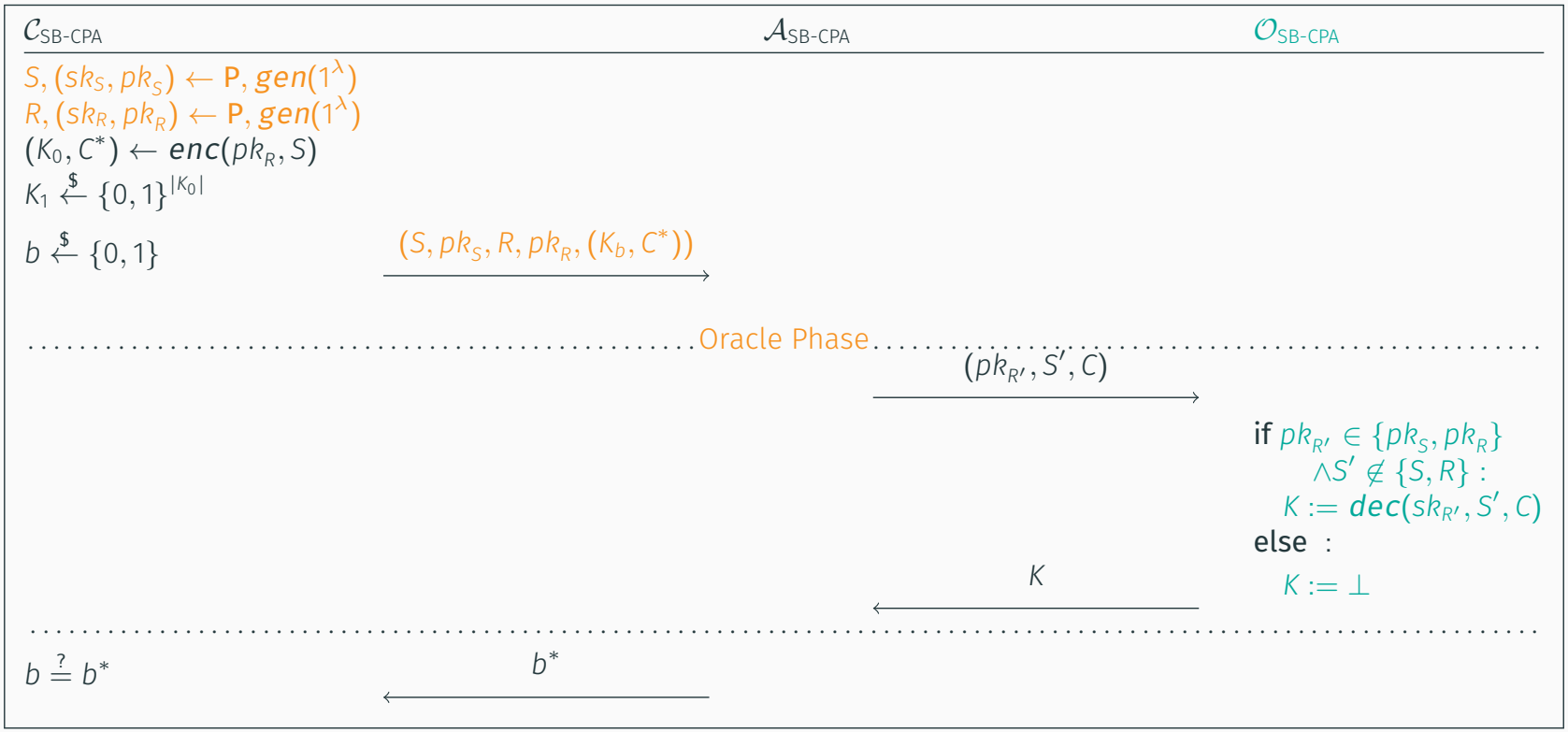
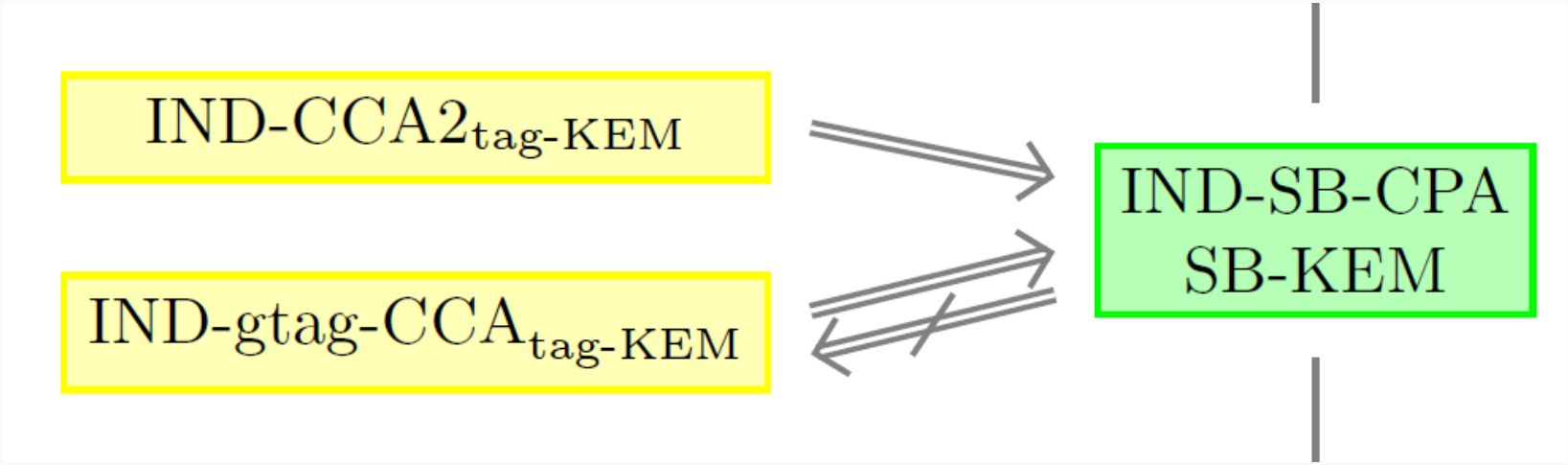



**Figure 1:** The IND-SB-CPA$_{\text{SB-KEM}}$ Game for SB-CPA$_{\text{SB-KEM}}$

# How weak is IND-SB-CPA$_{\text{SB-KEM}}$?

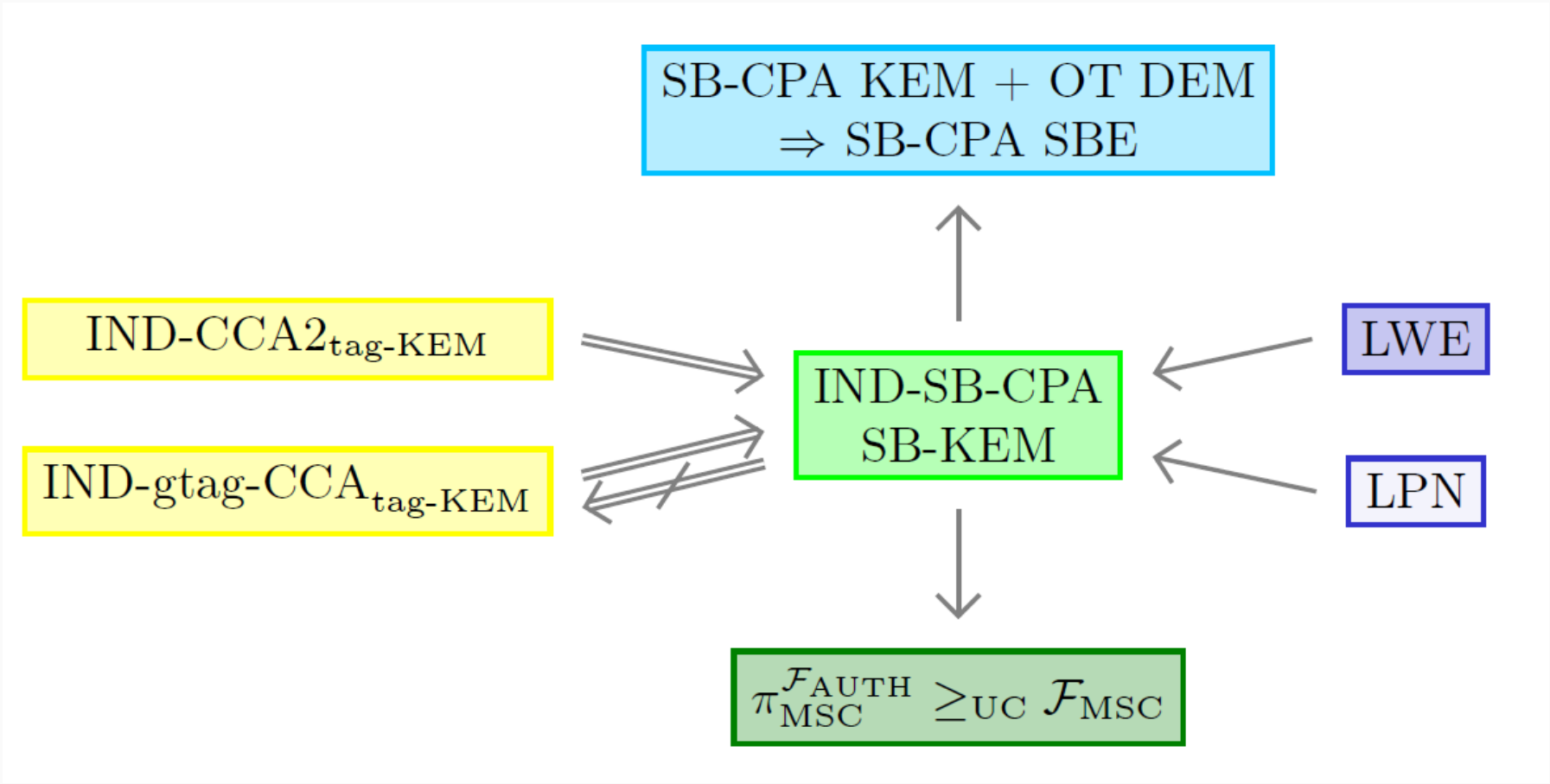


# Conclusion

# Frequent Misunderstandings

- IND-SB-CPA$_{\text{SB-KEM}}$ is **not** a replacement of CCA2
- IND-SB-CPA$_{\text{SB-KEM}}$ is **not** limited to constructions in the standard model

# Summary


SB-CPA KEM + OT DEM
⇒ SB-CPA SBE
IND-CCA2tag-KEM
IND-gtag-CCAtag-KEM
IND-SB-CPA
SB-KEM
LWE
LPN
$\pi_{\mathrm{MSC}}^{\mathcal{F}_{\mathrm{AUTH}}} \geq_{\mathrm{UC}} \mathcal{F}_{\mathrm{MSC}}$

Questions?

# References i


M. Abe, R. Gennaro, K. Kurosawa, and V. Shoup.
**Tag-kem/dem: A new framework for hybrid encryption and a new analysis of kurosawa-desmedt kem.**
In R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 128–146, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

W. Beskorovajnov, R. Gröll, J. Müller-Quade, A. Ottenhues, and R. Schwerdt.
**A new security notion for pkc in the standard model: Weaker, simpler, and still realizing secure channels.**
In G. Hanaoka, J. Shikata, and Y. Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 316–344, Cham, 2022. Springer International Publishing.

# References ii



R. Canetti.
**Universally composable security: A new paradigm for cryptographic protocols.**
In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.


R. Canetti, H. Krawczyk, and J. B. Nielsen.
**Relaxing chosen-ciphertext security.**
In D. Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, pages 565–582, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.


R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat, and V. Vaikuntanathan.
**Bounded cca2-secure encryption.**
In *ASIACRYPT*, volume 4833, pages 502–518. Springer, 2007.

# References iii



R. Cramer and V. Shoup.
**Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack.**
*SIAM Journal on Computing*, 33, 01 2002.


J. Herranz, D. Hofheinz, and E. Kiltz.
**Some (in)sufficient conditions for secure hybrid encryption.**
*Inf. Comput.*, 208:1243–1257, 11 2010.


D. Hofheinz and E. Kiltz.
**Secure hybrid encryption from weakened key encapsulation.**
In *Advances in Cryptology-CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings 27*, pages 553–571. Springer, 2007.

# References iv


S. Hohenberger, A. Lewko, and B. Waters.
**Detecting dangerous queries: A new approach for chosen ciphertext security.**
In *Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31*, pages 663–681. Springer, 2012.

K. Kurosawa and Y. Desmedt.
**A new paradigm of hybrid encryption scheme.**
In M. Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, pages 426–442, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

# References v


P. D. MacKenzie, M. K. Reiter, and K. Yang.
**Alternatives to non-malleability: Definitions, constructions, and applications (extended abstract).**
In M. Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 171–190. Springer Berlin Heidelberg, 2004.

W. Nagao, Y. Manabe, and T. Okamoto.
**A universally composable secure channel based on the kem-dem framework.**
volume 89-A, pages 28–38, 01 2006.

V. Shoup.
**A proposal for an iso standard for public key encryption.**
Cryptology ePrint Archive, Paper 2001/112, 2001.

# Summary

Get the source of this theme and the demo presentation from

*github.com/matze/mtheme*