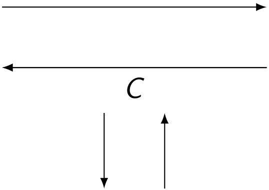
Kurosawa-Desmedt Meets Tight Security

Romain Gay (École normale supérieure)
Dennis Hofheinz (Karlsruhe Institute of Technology)
Lisa Kohl (Karlsruhe Institute of Technology)

Scenario

All illustrations by John Tenniel, Alice's Adventures in Wonderland, 1865.

Scenario



$(sk, pk) \leftarrow \mathbf{KeyGen}(1^\lambda)$

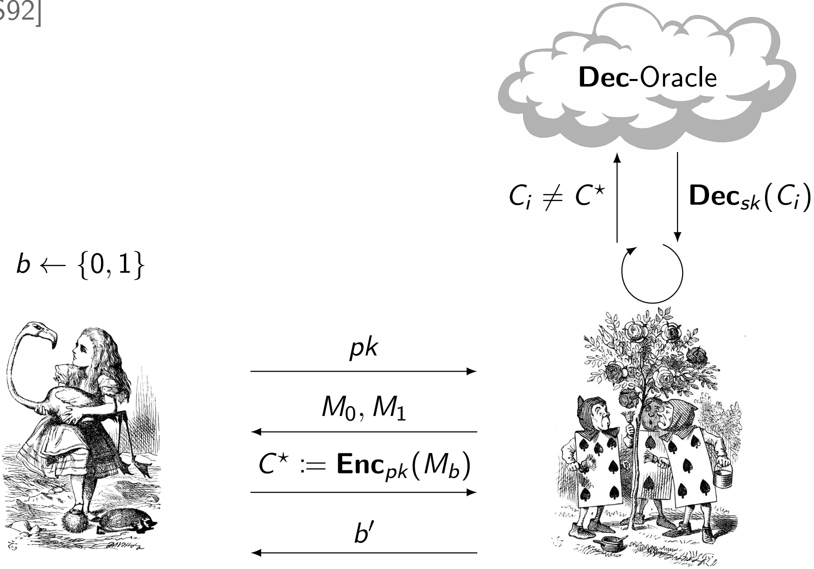
$M = \mathbf{Dec}_{sk}(C)$

$C \leftarrow \mathbf{Enc}_{pk}(M)$

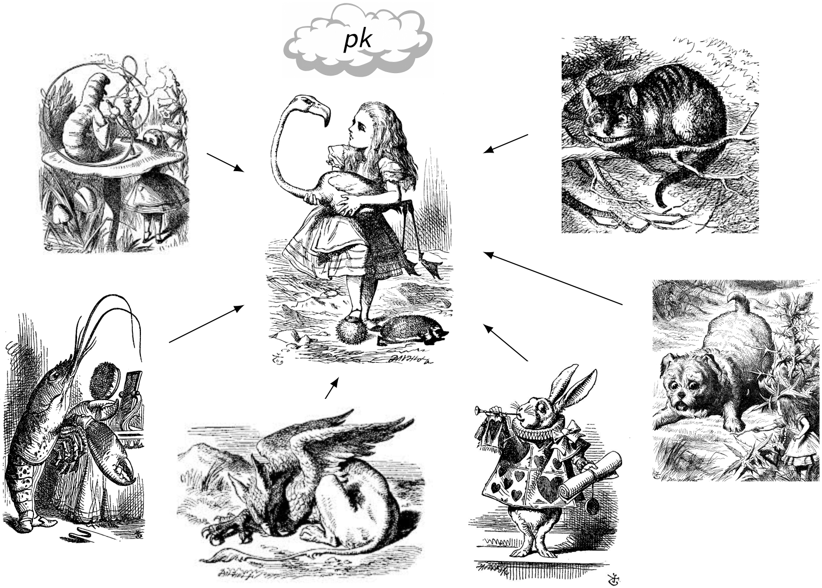
All illustrations by John Tenniel, Alice's Adventures in Wonderland, 1865.

Security model (IND-CCA)

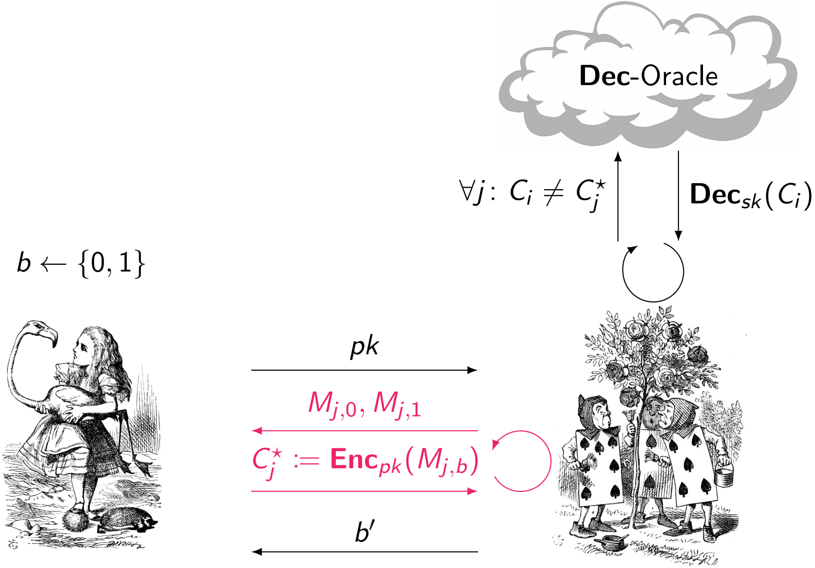
[RS92]



Multi-ciphertext scenario



Security model (Multi-ciphertext IND-CCA)



Tight security reductions
[BBM00],[HJ12]

breaks encryption w.
advantage ε

Tight security reductions

[BBM00],[HJ12]

breaks assumption w.
advantage ε/L
L = security loss

breaks encryption w.
advantage ε

Tight security reductions

[BBM00],[HJ12]

breaks assumption w.
advantage $2^{-128}/2^{30}$
L = security loss

breaks encryption w.
advantage 2^{-128}

Multi-ciphertext sec. via hybrid argument: $L \in \Omega(Q_{\mathbf{enc}})$

Tight security reductions

[BBM00],[HJ12]

breaks assumption w. advantage $2^{-128}/2^{30}$

L = security loss

breaks encryption w. advantage 2^{-128}

Multi-ciphertext sec. via hybrid argument: $L \in \Omega(Q_{\mathbf{enc}})$

(Almost) tight reduction: $L = c_{\text{small}} \cdot \lambda$

$\Rightarrow$ **shorter concrete parameters**

CCA-secure encryption schemes

	$\lvert C \rvert - \lvert M \rvert$	$\lvert pk \rvert$	assumption	w/o pairing	security loss
[CS98]	3	3	DDH	✓	$\Omega(Q)$
[KD04]	2	2	DDH	✓	$\Omega(Q)$
[HJ12]	$\Omega(\lambda)$	$\mathcal{O}(1)$	DLin	✗	$\mathcal{O}(1)$
[GHKW16]	3	2λ	DDH	✓	$\mathcal{O}(\lambda)$
[Hof17]	6	28	DLin	✗	$\mathcal{O}(\lambda)$

CCA-secure encryption schemes

	$\|C\| - \|M\|$	$\|pk\|$	assumption	w/o pairing	security loss
[CS98]	3	3	DDH	✓	$\Omega(Q)$
[KD04]	2	2	DDH	✓	$\Omega(Q)$
[HJ12]	$\Omega(\lambda)$	$\mathcal{O}(1)$	DLin	✗	$\mathcal{O}(1)$
[GHKW16]	3	2λ	DDH	✓	$\mathcal{O}(\lambda)$
[Hof17]	6	28	DLin	✗	$\mathcal{O}(\lambda)$
Ours	3	6	DDH	✓	$\mathcal{O}(\lambda)$

Our scheme

Kurosawa-Desmedt + OR-proof π (new!)

Our scheme

Kurosawa-Desmedt + OR-proof π (new!)

Questions:

1. What is π good for?
2. How does π look like?

Recap: Decisional Diffie-Hellman assumption

$\mathbb{G}$ group, $\mathbf{a} \in \mathbb{G}^2$

Diffie-Hellman language:

$$\mathcal{L}_{\mathbf{a}}^{\text{lin}} = \left\{ \mathbf{x} \in \mathbb{G}^2 \mid \exists w \in \mathbb{Z}_{|\mathbb{G}|} : \mathbf{x} = \mathbf{a} \cdot w \right\}$$

Recap: Decisional Diffie-Hellman assumption

$\mathbb{G}$ group, $\mathbf{a} \in \mathbb{G}^2$

Diffie-Hellman language:

$$\mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} = \left\{ \mathbf{x} \in \mathbb{G}^2 \mid \exists w \in \mathbb{Z}_{|\mathbb{G}|} : \mathbf{x} = \mathbf{a} \cdot w \right\}$$

DDH:

$$\left(\mathbf{a}, \mathbf{a} \cdot w \right) \approx_c \left(\mathbf{a}, \mathbf{u} \right)$$

Recap: Decisional Diffie-Hellman assumption

$\mathbb{G}$ group, $\mathbf{a} \in \mathbb{G}^2$

Diffie-Hellman language:

$$\mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} = \left\{ \mathbf{x} \in \mathbb{G}^2 \mid \exists w \in \mathbb{Z}_{|\mathbb{G}|} : \mathbf{x} = \mathbf{a} \cdot w \right\}$$

DDH:

$$\left(\mathbf{a}, \mathbf{a} \cdot w \right) \approx_c \left(\mathbf{a}, \mathbf{u} \right)$$

Useful for tightness: $\Downarrow$ Re-Randomizability $\Downarrow$

$$\left(\mathbf{a}, \mathbf{a} \cdot w_1, \mathbf{a} \cdot w_2, \cdots, \mathbf{a} \cdot w_n \right) \approx_c \left(\mathbf{a}, \mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n \right)$$

Recap: Hash proof system
[CS98]

Purpose: prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ to a designated verifier

Recap: Hash proof system
[CS98]

Purpose: prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ to a designated verifier

Completeness: $\forall \mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w:

$$\mathbf{PubH}(pk, \mathbf{x}, w) = \mathbf{PrivH}(sk, \mathbf{x})$$

1- **Universality:** $\forall \mathbf{x} \notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$

$$(pk, \mathbf{PrivH}(sk, \mathbf{x})) \approx_s (pk, \mathrm{rand})$$

Recap: Hash proof system

[CS98]

Purpose: prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ to a designated verifier

Completeness: $\forall \mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w:

$$\mathbf{PubH}(pk, \mathbf{x}, w) = \mathbf{PrivH}(sk, \mathbf{x})$$

1- **Universality:** $\forall \mathbf{x} \notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$

$$(pk, \mathbf{PrivH}(sk, \mathbf{x})) \approx_s (pk, \mathrm{rand})$$

Recap: Hash proof system

[CS98],[KD04]

Purpose: prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ to a designated verifier

Completeness: $\forall \mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w:

$$\mathbf{PubH}(pk, \mathbf{x}, w) = \mathbf{PrivH}(sk, \mathbf{x})$$

1- **Universality:** $\forall \mathbf{x} \notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$

$$(pk, \mathbf{PrivH}(sk, \mathbf{x})) \approx_s (pk, \mathrm{rand})$$

$$\mathbf{PubEval}(pk, \mathbf{x}, w) = \mathbf{PubH}(pk_1, \mathbf{x}, w) + \mathsf{H}(\mathbf{x}) \cdot \mathbf{PubH}(pk_2, \mathbf{x}, w),$$

H collision resistant hash function

Recap: Kurosawa-Desmedt and its proof
[KD04]

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}^{\mathrm{lin}}_{\mathbf{a}}$ with witness w
- compute $k = \mathbf{PubEval}(pk, \mathbf{x}, w)$
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}})$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- compute $\mathbf{D}_k(C_{sym})$

Recap: Kurosawa-Desmedt and its proof
[KD04]

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w
- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$ // Completeness
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}})$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- compute $\mathbf{D}_k(C_{sym})$

Recap: Kurosawa-Desmedt and its proof
[KD04]

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathbb{G}^2$ // DDH
- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$ // Completeness
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}})$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- compute $\mathbf{D}_k(C_{sym})$

Recap: Kurosawa-Desmedt and its proof

[KD04]

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathbb{G}^2$ // DDH
- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$ // Completeness
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}})$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- compute $\mathbf{D}_k(C_{sym})$

computational 2-universality $\Rightarrow$ reject decryption queries $\notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$

$\Rightarrow$ IND-CCA-security

Recap: Kurosawa-Desmedt and its proof

[KD04]

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathbb{G}^2$ // DDH
- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$ // Completeness
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}})$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- compute $\mathbf{D}_k(C_{sym})$

computational 2-universality $\Rightarrow$ reject decryption queries $\notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$

$\Rightarrow$ IND-CCA-security

Problem: entropy in *sk* limited $\Rightarrow$ reduction **non-tight**

Reminder: Our scheme

Kurosawa-Desmedt + OR-proof π (new!)

Security of our scheme

Idea: use freshly randomized *sk* for each ciphertext

$\xRightarrow[\text{of DDH}]{\text{re-randomizability}}$ randomize all ciphertexts at once [GHKW16]

Security of our scheme

Idea: use freshly randomized *sk* for each ciphertext

$\xrightarrow[\text{of DDH}]{\text{re-randomizability}}$ randomize all ciphertexts at once [GHKW16]

Difficulty: how to answer decryption queries?

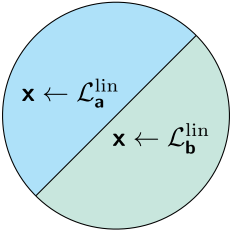
Security of our scheme

Idea: use freshly randomized *sk* for each ciphertext

$\overset{\text{re-randomizability}}{\underset{\text{of DDH}}{\Longrightarrow}}$ randomize all ciphertexts at once [GHKW16]

Difficulty: how to answer decryption queries?

Idea: first randomize *sk* step-by-step [GHKW16], [Hof17]



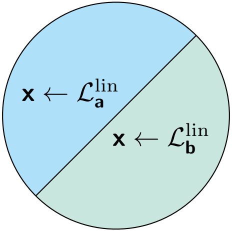
Security of our scheme

Idea: use freshly randomized *sk* for each ciphertext

$\overset{\text{re-randomizability}}{\underset{\text{of DDH}}{\Longrightarrow}}$ randomize all ciphertexts at once [GHKW16]

Difficulty: how to answer decryption queries?

Idea: first randomize *sk* step-by-step [GHKW16], [Hof17]



Difficulty: have to ensure $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$ in **Dec**-queries

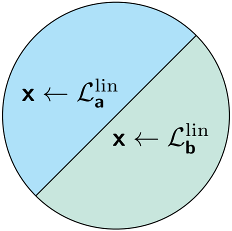
Security of our scheme

Idea: use freshly randomized *sk* for each ciphertext

$\overset{\text{re-randomizability}}{\underset{\text{of DDH}}{\Longrightarrow}}$ randomize all ciphertexts at once [GHKW16]

Difficulty: how to answer decryption queries?

Idea: first randomize *sk* step-by-step [GHKW16], [Hof17]



Difficulty: have to ensure $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\text{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\text{lin}}$ in **Dec**-queries

Idea: use explicit proof π [Hof17], **but** w/o pairings

Our scheme (simplified)

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$
- compute $k = \mathbf{PubEval}(pk, \mathbf{x}, w)$
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}}, \pi)$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}, \pi))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- if π valid compute $\mathbf{D}_k(C_{sym})$ else $\perp$

Our scheme (simplified)

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\text{lin}}$ with witness w, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\text{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\text{lin}}$
- compute $k = \mathbf{PubEval}(pk, \mathbf{x}, w)$
- publish $C = (\mathbf{x}, \underbrace{\mathbf{E}_k(M)}_{=C_{sym}}, \pi)$

$\mathbf{Dec}_{sk}(C = (\mathbf{x}, C_{sym}, \pi))$:

- compute $k = \mathbf{PrivEval}(sk, \mathbf{x})$
- if π valid compute $\mathbf{D}_k(C_{sym})$ else $\perp$

Main challenge: construct **pairing-free** non-interactive OR-proof

OR-proof

Goal: efficient pairing-free proof for $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

OR-proof

Goal: efficient pairing-free proof for $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

Observation: honest proof generation for $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ sufficient

$\Rightarrow$ employ **hash proof system**

OR-proof

Goal: efficient pairing-free proof for $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

$\mathbf{Enc}_{pk}(M)$:

- choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ with witness w, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

Observation: honest proof generation for $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$ sufficient

$\Rightarrow$ employ **hash proof system**

But: during randomization of *sk*

- sometimes choose $\mathbf{x} \leftarrow_R \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$, prove $\mathbf{x} \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$

Difficulty: forging a proof for $\mathbf{x} \notin \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}} \cup \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$ must remain hard

OR-proof

Solution: protect hash proof system by encrypting its evaluation

- $\mathsf{enc}_{\mathbf{x}}$ encryption scheme depending on $\mathbf{x}$
- $\mathsf{enc}_{\mathbf{x}}$ will be **lossy** for $\mathbf{x} \in \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$:

$$\forall \mathbf{x} \in \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}, \forall k \in \mathbb{Z}_{|\mathbb{G}|} : \mathsf{enc}_{\mathbf{x}}(k) \approx_s \mathsf{enc}_{\mathbf{x}}(\mathrm{rand})$$

OR-proof

Solution: protect hash proof system by encrypting its evaluation

- $\mathbf{enc_x}$ encryption scheme depending on $\mathbf{x}$
- $\mathbf{enc_x}$ will be **lossy** for $\mathbf{x} \in \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}$:

$$\forall \mathbf{x} \in \mathcal{L}_{\mathbf{b}}^{\mathrm{lin}}, \forall k \in \mathbb{Z}_{|\mathbb{G}|} : \mathbf{enc_x}(k) \approx_s \mathbf{enc_x}(\mathrm{rand})$$

Our OR-proof:

- $\mathbf{x} = \mathbf{a} \cdot w \in \mathcal{L}_{\mathbf{a}}^{\mathrm{lin}}$:

$$\pi = \mathbf{enc_x}(\mathbf{PubH}(pk, \mathbf{x}, w))$$

Conclusion

	$\lvert C\rvert - \lvert M\rvert$	$\lvert pk\rvert$	assumption	w/o pairing	security loss
[CS98]	3	3	DDH	✓	$\mathcal{O}(Q)$
[KD04]	2	2	DDH	✓	$\mathcal{O}(Q)$
[HJ12]	$\Omega(\lambda)$	$\mathcal{O}(1)$	DLin	✗	$\mathcal{O}(1)$
[GHKW16]	3	2λ	DDH	✓	$\mathcal{O}(\lambda)$
[Hof17]	6	28	DLin	✗	$\mathcal{O}(\lambda)$
Ours	3	6	DDH	✓	$\mathcal{O}(\lambda)$

Key building block: new efficient pairing-free NIDV OR-proof

Thank you!

Conclusion

	$\lvert C\rvert - \lvert M\rvert$	$\lvert pk\rvert$	assumption	w/o pairing	security loss
[CS98]	3	3	DDH	✓	$\mathcal{O}(Q)$
[KD04]	2	2	DDH	✓	$\mathcal{O}(Q)$
[HJ12]	$\Omega(\lambda)$	$\mathcal{O}(1)$	DLin	✗	$\mathcal{O}(1)$
[GHKW16]	3	2λ	DDH	✓	$\mathcal{O}(\lambda)$
[Hof17]	6	28	DLin	✗	$\mathcal{O}(\lambda)$
Ours	3	6	DDH	✓	$\mathcal{O}(\lambda)$

Key building block: new efficient pairing-free NIDV OR-proof

Thank you!

Bibliography I

Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements". In: *EUROCRYPT 2000*. Ed. by Bart Preneel. Vol. 1807. LNCS. Springer, Heidelberg, May 2000, pp. 259–274.

Ronald Cramer and Victor Shoup. "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack". In: *CRYPTO'98*. Ed. by Hugo Krawczyk. Vol. 1462. LNCS. Springer, Heidelberg, Aug. 1998, pp. 13–25.

Bibliography II

Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. "Tightly CCA-Secure Encryption Without Pairings". In: *EUROCRYPT 2016, Part I*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9665. LNCS. Springer, Heidelberg, May 2016, pp. 1–27. DOI: 10.1007/978-3-662-49890-3_1.

Dennis Hofheinz and Tibor Jager. "Tightly Secure Signatures and Public-Key Encryption". In: *CRYPTO 2012*. Ed. by Reihaneh Safavi-Naini and Ran Canetti. Vol. 7417. LNCS. Springer, Heidelberg, Aug. 2012, pp. 590–607.

Bibliography III

Dennis Hofheinz. “Adaptive Partitioning”. In: *EUROCRYPT 2017, Part III*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Cham: Springer International Publishing, 2017, pp. 489–518.

Kaoru Kurosawa and Yvo Desmedt. “A New Paradigm of Hybrid Encryption Scheme”. In: *CRYPTO 2004*. Ed. by Matthew Franklin. Vol. 3152. LNCS. Springer, Heidelberg, Aug. 2004, pp. 426–442.

Charles Rackoff and Daniel R. Simon. “Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack”. In: *CRYPTO’91*. Ed. by Joan Feigenbaum. Vol. 576. LNCS. Springer, Heidelberg, Aug. 1992, pp. 433–444.