Innovative R&D by NTT

Improving Practical UC-Secure Commitments based on the DDH Assumption

Eiichiro Fujisaki (藤崎 英一郎)

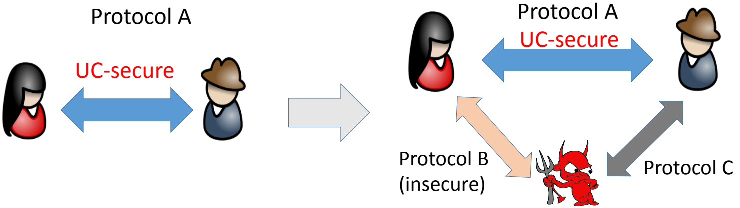
NTT Secure Platform Laboratories

10th Conference on Security and Cryptography for Networks, on Sept. 1st 2016

Agenda

Motivation: Efficient UC-Secure Protocols

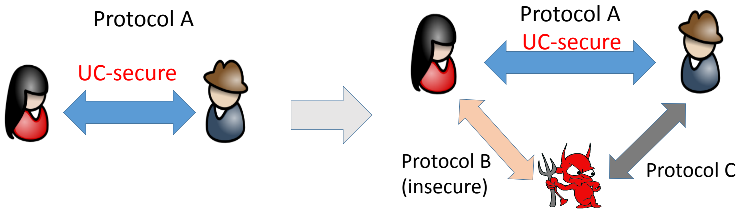
Universal composability (UC) framework guarantees that if a protocol is proven secure in the UC framework, it remains secure even if it is run concurrently with *arbitrary* protocols.



Weak spot: The lack of *efficient* instantiations.

Motivation: Efficient UC-Secure Protocols

Universal composability (UC) framework guarantees that if a protocol is proven secure in the UC framework, it remains secure even if it is run concurrently with *arbitrary* protocols.



Weak spot: The lack of *efficient* instantiations.

Why UC Commitments ?

Why UC Commitments ?

Because **UC commitments are complete.**

Why UC Commitments ?

Because **UC commitments are complete.**

UC commitments **imply** UC zero-knowledge protocols and UC multi-party computations (MPC) [CLOS02].

Why UC Commitments ?

Because **UC commitments are complete.**

UC commitments **imply** UC zero-knowledge protocols and UC multi-party computations (MPC) [CLOS02].

More efficient (static/adaptively) UC-secure commitment scheme enables *more efficient* constructions of (static/adaptively) UC-secure (MPC) protocols.

UC Commitments [CF01]

Informally, a commitment scheme is UC-secure if the **hiding** and **binding** properties hold *even if it runs concurrently with arbitrary protocols*.

For a technical reason, we make a commitment scheme **extractable, equivocal and con-current non-malleable**. Then, prove that it is universally composable.

UC Commitments [CF01]

Informally, a commitment scheme is UC-secure if the **hiding** and **binding** properties hold *even if it runs concurrently with arbitrary protocols*.

For a technical reason, we make a commitment scheme **extractable, equivocal and con-current non-malleable**. Then, prove that it is universally composable.

Static and Adaptive UC Security

- **Static UC-security** = UC security against **static corruption**.
- **Adaptive UC-security** with/out erasure = UC security against **adaptive corruption** with/out erasure.

- **Static Corruption**: An adversary should decide to corrupt parties only before a protocol starts.
- **Adaptive Corruption**: An adversary may corrupt parties at any timing.
- **Secure Erasure**: Honest parties can securely erase their unnecessary inner states.

Agenda

1 Motivation

2 Previous Work

3 Our Result

4 Idea of Improvement

5 Proof Outline (Static case)

6 Static to Adaptive

7 Conclusion

Previous Work

- [CF01]
  - Seminal paper. Non-interactive, reusable, adaptively UC-secure without erasure (= fully-equipped).
- [CLOS02]
  - From general assumption, fully-equipped but Inefficient.
- [DN02, DG03, NFT12, Fuj14]
  - **Efficient adaptively** UC-secure without erasure (based on N^d modulus for $d \geq 2$). [NFT12]: one-time. [Fuj14]: fully-equipped.
- [Lin11, BCPV13], [FLM11]
  - **Efficient adaptively** UC-secure *with erasure* (based on prime order groups). [FLM11]: non-interactive (based on *bilinear* groups).
- [GIKW14, DDGN14, CDD$^+$15, FJNT16, CDD$^+$16]
  - Fast, statistic UC-secure.
- [DSW08]
  - Global UC-secure.
- [HM04, CJS14]
  - Random oracle model.

NTT

Previous Work

- [CF01]
  - Seminal paper. Non-interactive, reusable, adaptively UC-secure without erasure (= fully-equipped).
- [CLOS02]
  - From general assumption, fully-equipped but Inefficient.
- [DN02, DG03, NFT12, Fuj14]
  - **Efficient adaptively** UC-secure without erasure (based on N^d modulus for $d \geq 2$). [NFT12]: one-time. [Fuj14]: fully-equipped.
- [Lin11, BCPV13], [FLM11]
  - **Efficient adaptively** UC-secure *with erasure* (based on prime order groups). [FLM11]: non-interactive (based on *bilinear* groups).
- [GIKW14, DDGN14, CDD$^+$15, FJNT16, CDD$^+$16]
  - Fast, statistic UC-secure.
- [DSW08]
  - Global UC-secure.
- [HM04, CJS14]
  - Random oracle model.

NTT

Efficient Adaptively UC-secure with Erasure

So far, [BCPV13] provides the most efficient adaptively UC-secure commitment scheme.

- [Lin11]: Static and adaptively UC-secure interactive commitment schemes based on an *arbitrary* cyclic group on which the DDH assumption holds.
- [BCPV13]: Improvement of [Lin11]. Reduce round, communication, and computational complexities. Fix a bug of Lindell's adaptively UC-secure commitment scheme.

[BCPV13]: Blazy, Chevalier, Pointcheval, and Vergnaud (ACNS2013).

Agenda

Our Result

Further improve efficiency of [BCPV13] *in both static and adaptive cases* under the *same* assumption.

- Improvement: CRS size, communication complexity, and computational complexity.
- Round complexity: same as [BCPV13].
- As the previous works, work on an arbitrary cyclic group on which the DDH assumption holds true.

NTT

Comparison

Table: Comparison among the UC commitments based on the DDH assumption (along with the collision resistant hash functions).

Schemes	CRS	Communication Complexity	Computational Complexity	Rounds Com/Decom	Security
Lin11 [Lin11, § 3]	$7\lvert\mathbb{G}\rvert$	$10\lvert\mathbb{G}\rvert + 4\kappa$	$27T^{\mathsf{exp}}(\mathbb{G})$	1/4	Static
Lin11 [Lin11, § 4]	$8\lvert\mathbb{G}\rvert$	$12\lvert\mathbb{G}\rvert + 6\kappa$	$36T^{\mathsf{exp}}(\mathbb{G})$	5/1	Adaptive
BCPV13 [BCPV13, § 5.1]	$7\lvert\mathbb{G}\rvert$	$9\lvert\mathbb{G}\rvert + 3\kappa$	$22T^{\mathsf{exp}}(\mathbb{G})$	1/3	Static
BCPV13 [BCPV13, § 5.3]	$7\lvert\mathbb{G}\rvert$	$10\lvert\mathbb{G}\rvert + 4\kappa$	$26T^{\mathsf{exp}}(\mathbb{G})$	3/1	Adaptive
Ours (Static)	$5\lvert\mathbb{G}\rvert$	$7\lvert\mathbb{G}\rvert + 3\kappa$	$18T^{\mathsf{exp}}(\mathbb{G})$	1/3	Static
Ours (Adaptive)	$5\lvert\mathbb{G}\rvert$	$7\lvert\mathbb{G}\rvert + 3\kappa$	$18T^{\mathsf{exp}}(\mathbb{G})$	3/1	Adaptive

Note: All *adaptively* UC-secure commitments above assume *secure erasure*.

Agenda

UC Commitments are required

Extractable

A simulator can extract the value that a corrupted party commits to.

Equivocal

A simulator can produce commitments that can be opened to any value.

When executing extraction and equivocation, the simulator is not allowed to rewind the adversary.

Concurrently Non-Malleable

An adversary must not be able to create commitments that are related to commitments generated by honest parties.

High-Level Idea (Static) by Lindell

- The commit phase:
  - Use PKE. Send $\mathrm{CT} = \mathbf{E}_{pk}(x; w)$ as a commitment (for extractability).
- The open phase:
  - Open x and prove that CT *is a proper ciphertext of* x in a zero-knowledge manner (for equvocality).
- For concurrent Non-Malleability:
  - Trivial solusion: Use IND-CCA secure (= static UC secure) PKE and UC zero-knowledge.
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.

Lindell's Static UC-Secure Commitments

- Trivial solusion : IND-CCA PKE (for commitment) + UC zero-knowledge proofs (of knowledge) (for opening).
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.

Lindell's Static UC-Secure Commitments

- Trivial solusion : IND-CCA PKE (for commitment) + UC zero-knowledge proofs (of knowledge) (for opening).
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.
- Lindell's Observation: IND-CCA PKE + straight-line simulatable zero-knowledge proof on language (*).

Lindell's Static UC-Secure Commitments

- Trivial solusion : IND-CCA PKE (for commitment) + UC zero-knowledge proofs (of knowledge) (for opening).
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.
- Lindell's Observation: IND-CCA PKE + straight-line simulatable zero-knowledge proof on language (*).
  - (*): 4-round implementation using dual mode encryption + Sigma protocol (by Lindell).

BCPV Static UC-Secure Commitments

- Trivial solusion : IND-CCA PKE (for commitment) + UC zero-knowledge proofs (of knowledge) (for opening).
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.
- Lindell's Observation: IND-CCA PKE + straight-line simulatable zero-knowledge proof on language (*).
  - (*): 4-round implementation using dual mode encryption + Sigma protocol (by Lindell).
  - (*): 3-round implementation using trapdoor commitment + Sigma protocol (by BCPV).

NTT

BCPV Static UC-Secure Commitments

- Trivial solusion : IND-CCA PKE (for commitment) + UC zero-knowledge proofs (of knowledge) (for opening).
  - Problem: UC zero-knowledge proofs are constructed from UC commitments.
- Lindell's Observation: IND-CCA PKE + straight-line simulatable zero-knowledge proof on language (*).
  - (*): 4-round implementation using dual mode encryption + Sigma protocol (by Lindell).
  - (*): 3-round implementation using trapdoor commitment + Sigma protocol (by BCPV).
    - = [Dam00]: Efficient concurrent zero-knowledge in auxiliary string model.

Our static UC-Secure Commitment

UC zero knowledge can be weaker. Then, how about IND-CCA PKE ?

Our static UC-Secure Commitment

UC zero knowledge can be weaker. Then, how about IND-CCA PKE ?

Can replace IND-CCA PKE with IND-PCA PKE ($\star$).

$\star$: The Short Cramer-Shoup encryption [ABP15].

Our Observation

- IND-CCA PKE is overkill in both static and adaptive cases.
  - **Can replace IND-CCA PKE with IND-PCA PKE**, where IND-PCA means semantical security against *plaintext checkable* attacks [ABP15].
- In the adaptive case, **two trapdoor commitments (w.r.t. two independent public-keys) can be reduced to a single trapdoor commitment**.

Agenda

Our static UC-Secure Commitment

Alice (Committer)		Bob (Receiver)
	The Commit Phase	
Commit to x by sending $\mathrm{CT} = \mathbf{E}^{pca}_{\mathrm{pk}^{\mathrm{enc}}}(x; w)$ (cf. BCPV13: IND-CCA)	$\xrightarrow{\mathrm{CT}}$	
	The Open Phase	
Open to x as follows: $\psi = \mathrm{Com}^{\mathrm{tc}}_{\mathrm{pk}^{\mathrm{tc}}}(\alpha; r_{\mathrm{tc}})$	$\xrightarrow{x,\ \psi}$	
	$\xleftarrow{\beta}$	$\beta \leftarrow \{0,1\}^{\lambda_{\mathrm{ch}}}$.
Compute γ using w. Reveal α with r_{tc}.	$\xrightarrow{\alpha, r_{\mathrm{tc}}, \gamma}$	Accept if (α, β, γ) is valid on (x, CT).

The open phase: a proof that "CT is a proper ciphetext of x."

Proof Outline

Environment $\mathcal{Z}$'s view: $(\mathsf{CT}, x, \rho, \mathsf{CT}', x', \rho', \tilde{x})$.

Table: The man-in-the-midle attack in the hybrid games

Games	Left Interaction Alice $\xrightarrow{(\mathsf{CT}, x, \rho)}$ Eve (corrupted)	Right Interaction Eve (corrupted) $\xrightarrow{(\mathsf{CT}', x', \rho')}$ Bob	Output to $\mathcal{Z}$ $\xrightarrow{\tilde{x}}$ $\mathcal{Z}$ (Env.)
G_0 (Real)	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = x'$
G_1	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_2	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and simulated proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_3 (Ideal)	Commit phase: $\mathsf{CT} = \mathbf{E}(0; w)$ Open phase: x and simulated proof ρ on the (false) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$

Statement T: CT is a proper ciphertext of x, i.e., $\mathsf{CT} = \mathbf{E}(x)$.
Statement T': CT' is a proper ciphertext of x', i.e., $\mathsf{CT}' = \mathbf{E}(x')$.

NTT

Proof Outline

Environment $\mathcal{Z}$'s view: $(\mathsf{CT}, x, \rho, \mathsf{CT}', x', \rho', \tilde{x})$.

Table: The man-in-the-midle attack in the hybrid games

Games	Left Interaction Alice $\stackrel{(\mathsf{CT},x,\rho)}{\longrightarrow}$ Eve (corrupted)	Right Interaction Eve (corrupted) $\stackrel{(\mathsf{CT}',x',\rho')}{\longrightarrow}$ Bob	Output to $\mathcal{Z}$ $\stackrel{\tilde{x}}{\longrightarrow} \mathcal{Z}$ (Env.)
G_0 (Real)	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = x'$
G_1	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_2	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and simulated proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_3 (Ideal)	Commit phase: $\mathsf{CT} = \mathbf{E}(0; w)$ Open phase: x and simulated proof ρ on the (false) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$

$G_0 \stackrel{c}{\approx} G_1$: By soundness property of ordinary zero-knowledge protocols and correctness of PKE.

Proof Outline

Environment $\mathcal{Z}$'s view: $(\mathsf{CT}, x, \rho, \mathsf{CT}', x', \rho', \tilde{x})$.

Table: The man-in-the-midle attack in the hybrid games

Games	Left Interaction Alice $\xrightarrow{(\mathsf{CT}, x, \rho)}$ Eve (corrupted)	Right Interaction Eve (corrupted) $\xrightarrow{(\mathsf{CT}', x', \rho')}$ Bob	Output to $\mathcal{Z}$ $\xrightarrow{\tilde{x}}$ $\mathcal{Z}$ (Env.)
G_0 (Real)	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = x'$
G_1	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_2	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and simulated proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_3 (Ideal)	Commit phase: $\mathsf{CT} = \mathbf{E}(0; w)$ Open phase: x and simulated proof ρ on the (false) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$

$G_1 \equiv G_2$: By perfect straight-line zero-knowledge simulator of [Dam00].

Proof Outline

Environment $\mathcal{Z}$'s view: $(\mathsf{CT}, x, \rho, \mathsf{CT}', x', \rho', \tilde{x})$.

Table: The man-in-the-midle attack in the hybrid games

Games	Left Interaction Alice $\xrightarrow{(\mathsf{CT}, x, \rho)}$ Eve (corrupted)	Right Interaction Eve (corrupted) $\xrightarrow{(\mathsf{CT}', x', \rho')}$ Bob	Output to $\mathcal{Z}$ $\xrightarrow{\tilde{x}}$ $\mathcal{Z}$ (Env.)
G_0 (Real)	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = x'$
G_1	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and real proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_2	Commit phase: $\mathsf{CT} = \mathbf{E}(x; w)$ Open phase: x and simulated proof ρ on the (true) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$
G_3 (Ideal)	Commit phase: $\mathsf{CT} = \mathbf{E}(0; w)$ Open phase: x and simulated proof ρ on the (false) statement T	Commit phase: CT' Open phase: x' and proof ρ' on the statement T'	$\tilde{x} = \mathbf{D}_{sk}(\mathsf{CT}')$

$G_2 \overset{c}{\approx} G_3$: By IND-PCA secure PKE. Construct A that breaks IND-PCA PKE using $\mathcal{Z}$ and corrupted Eve.

Proof between G_2 and G_3

Tricky part: A is *only given the plaintext-checkable (PCA) oracle, not the decryption oracle*.

The decryption oracle seems to be needed, because the simulator needs the decryption of ciphertexts from Eve. However, **it is not true**.

Proof between G_2 and G_3

Tricky part: A is *only given the plaintext-checkable (PCA) oracle, not the decryption oracle*.

The decryption oracle seems to be needed, because the simulator needs the decryption of ciphertexts from Eve. However, **it is not true**.

- Case1 (Eve **always opens commitments correctly**). Then A can perfectly **simulate $\mathcal{Z}$'s views** in G_2 and G_3, according as given $\mathrm{CT} = \mathbf{E}(x)$ and $\mathbf{E}(0)$ **without knowing** sk. Then, "the advantage of A" = "the advantage of $\mathcal{Z}$".

Proof between G_2 and G_3

Tricky part: A is *only given the plaintext-checkable (PCA) oracle, not the decryption oracle*.

The decryption oracle seems to be needed, because the simulator needs the decryption of ciphertexts from Eve. However, **it is not true**.

- Case1 (Eve **always opens commitments correctly**). Then A can perfectly **simulate $\mathcal{Z}$'s views** in G_2 and G_3, according as given $\mathrm{CT} = \mathbf{E}(x)$ and $\mathbf{E}(0)$ **without knowing** sk. Then, "the advantage of A" = "the advantage of $\mathcal{Z}$".
- Case 2 (Eve **opens commitment wrongly**). Then A must play in G_3, because **in G_2, Eve cannot fool the receiver**. A can check if she fooled the receiver or not, **using the PCA oracle**. Then, A can halt and say "I am playing in G_3".

Agenda

1 Motivation

2 Previous Work

3 Our Result

4 Idea of Improvement

5 Proof Outline (Static case)

6 Static to Adaptive

7 Conclusion

Static to Adaptive

- Lindell's Idea: Switch the order of the messages (For soundness, commits to CT at the beginning).
- (BCPV's bug fix: Commit to (x, CT), not only CT to fix the statement for proof beforehand.)
- Our observation: CT and α (the first message of the Sigma protocol) can be committed to in the same commitment.

Static to Adaptive

- Lindell's Idea: Switch the order of the messages (For soundness, commits to CT at the beginning).
- (BCPV's bug fix: Commit to (x, CT), not only CT to fix the statement for proof beforehand.)
- Our observation: CT and α (the first message of the Sigma protocol) can be committed to in the same commitment.
  - *Can reduce communication and computational complexities*.

NTT

Our adaptively UC-Secure Commitment

Alice (Committer) | Bob (Receiver)

The Commit Phase

$\mathsf{CT} = \mathbf{E}^{pca}_{\mathsf{pk}^{\mathsf{enc}}}(x; w)$

$\psi = \mathsf{Com}^{\mathsf{tc}}_{\mathsf{pk}^{\mathsf{tc}}}((x, \mathsf{CT}, \alpha); r_{\mathsf{tc}})$ $\xrightarrow{\psi}$

$\xleftarrow{\beta}$ $\beta \leftarrow \{0,1\}^{\lambda_{\mathsf{ch}}}$.

Compute γ using w.

Erase w. $\xrightarrow{\mathsf{CT}}$

The Open Phase

Reveal (α, γ) with r_{tc}. $\xrightarrow{x,\ \alpha, r_{\mathsf{tc}}, \gamma}$ Accept if (α, β, γ) is valid on (x, CT).

Agenda

Conclusion

- We further improve *efficiency* of [BCPV13] *in both static and adaptive-with-erasure cases*.
- As with [Lin11, BCPV13], our proposals work on *an arbitrary cyclic group* on which the DDH assumption holds true.
- Our *adaptive* one is the *most efficient* adaptively UC-secure (with erasure) commitment scheme.

Thank you!

(Nearly) full version available at ePrint Archive 2016/656.

References I

[ABP15] Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.
Public-key encryption indistinguishable under plaintext-checkable attacks.
In Katz [Kat15], pages 332–352.

[BCPV13] Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud.
Analysis and improvement of lindell's uc-secure commitment schemes.
In Michael J. Jacobson, Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *ACNS 2013*, volume 7954 of *Lecture Notes in Computer Science*, pages 534–551. Springer, Heidelberg, 2013.

[Blu82] Manuel Blum.
Coin flipping by telephone - A protocol for solving impossible problems.
In *COMPCON'82, Digest of Papers, Twenty-Fourth IEEE Computer Society International Conference, San Francisco, California, USA, February 22-25, 1982*, pages 133–137, 1982.

[CDD+15] Ignacio Cascudo, Ivan Damgård, Bernardo Machado David, Irene Giacomelli, Jesper Buus Nielsen, and Roberto Trifiletti.
Additively homomorphic UC commitments with optimal amortized overhead.
In Katz [Kat15], pages 495–515.

[CDD+16] Ignacio Cascudo, Ivan Damgård, Bernardo David, Nico Döttling, and Jesper Buus Nielsen.
Rate-1, linear time and additively homomorphic UC commitments.
IACR Cryptology ePrint Archive, 2016:137, 2016.

[CF01] Ran Canetti and Marc Fischlin.
Universally composable commitments.
In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 19–40. Springer, Heidelberg, 2001.

References II

[CJS14] Ran Canetti, Abhishek Jain, and Alessandra Scafuro.
Practical UC security with a global random oracle.
In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *CCS 2014*, pages 597–608. ACM, 2014.

[CLOS02] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai.
Universally composable two-party and multi-party secure computation.
In *STOC 2002*, pages 494–503. ACM, 2002.
The full version available at `http://eprint.iacr.org/2002/140`.

[Dam00] Ivan Damgard.
Efficient concurrent zero-knowledge in auxiliary string model.
In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 418–430. Springer, Heidelberg, 2000.

[DDGN14] Ivan Damgård, Bernardo Machado David, Irene Giacomelli, and Jesper Buus Nielsen.
Compact VSS and efficient homomorphic UC commitments.
In Sarkar and Iwata [SI14], pages 213–232.

[DG03] Ivan Damgård and Jens Groth.
Non-interactive and reusable non-malleable commitment schemes.
In *STOC 2003*, pages 426–437. ACM, 2003.

[DN02] Ivan Damgård and Jesper Buus Nielsen.
Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor.
In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 581–596. Springer, Heidelberg, 2002.
The full version is available at `http://www.brics.dk/RS/01/41/`.

References III

[DSW08] Yevgeniy Dodis, Victor Shoup, and Shabsi Walfish.
Efficient constructions of composable commitments and zero-knowledge proofs.
In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 515–535. Springer, Heidelberg, 2008.

[FJNT16] Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen, and Roberto Trifiletti.
On the complexity of additively homomorphic UC commitments.
In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A (1)*, volume 9562 of *Lecture Notes in Computer Science*, pages 542–565. Springer, Heidelberg, 2016.

[FLM11] Marc Fischlin, Benoît Libert, and Mark Manulis.
Non-interactive and re-usable universally composable string commitments with adaptive security.
In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 468–485. Springer, Heidelberg, 2011.

[Fuj14] Eiichiro Fujisaki.
All-But-Many encryption - A new framework for fully-equipped UC commitments.
In Sarkar and Iwata [SI14], pages 426–447.

[GIKW14] Juan A. Garay, Yuval Ishai, Ranjit Kumaresan, and Hoeteck Wee.
On the complexity of UC commitments.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 677–694. Springer, Heidelberg, 2014.

[HM04] Dennis Hofheinz and Jörn Müller-Quade.
Universally composable commitments using random oracles.
In Moni Naor, editor, *TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 58–76. Springer, Heidelberg, 2004.

NTT

References IV

[Kat15] Jonathan Katz, editor.
Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings, volume 9020 of *Lecture Notes in Computer Science*. Springer, Heidelberg, 2015.

[Lin11] Yehuda Lindell.
Highly-efficient universally-composable commitments based on the DDH assumption.
In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 446–466. Springer, Heidelberg, 2011.
The full version available at at Cryptology ePrint Archive http://eprint.iacr.org/2011/180.

[NFT12] Ryo Nishimaki, Eiichiro Fujisaki, and Keisuke Tanaka.
An efficient non-interactive universally composable string-commitment scheme.
IEICE Transactions, 95-A(1):167–175, 2012.

[SI14] Palash Sarkar and Tetsu Iwata, editors.
Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II, volume 8874 of *Lecture Notes in Computer Science*. Springer, Heidelberg, 2014.