De Cifris Trends
in
Cryptographic Protocols

University of Trento and *De Componendis Cifris*

16 October 2023

Lecture 4

Dario Fiore **IMDEA Software Institute, Madrid, Spain**

Vector Commitments

Dario Fiore

IMDEA Software Institute, Madrid, Spain

Dario Fiore

Current position: Associate Research Professor
IMDEA Software Institute, Madrid, Spain

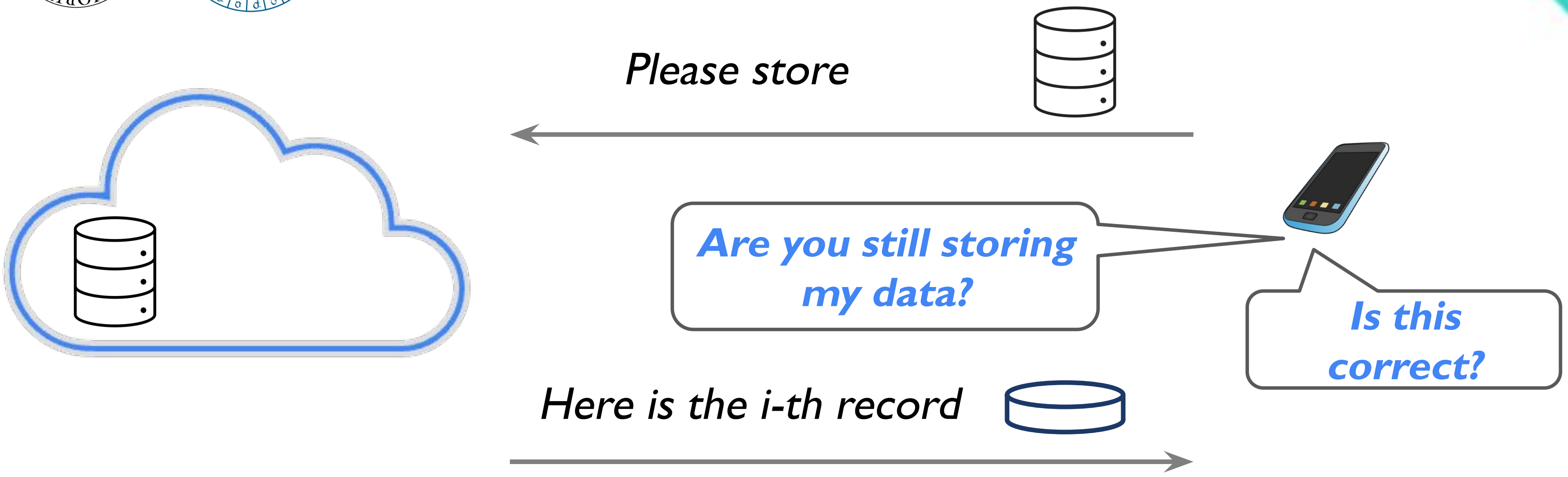
Short bio

- 2007-2010: **PhD** in Computer Science - University of Catania
- 2010-2013: **Postdoc** - ENS Paris, New York University,
  Max Planck Institute for Software Systems
- 2013-2019: Assistant Research Professor - IMDEA Software Institute

Research interests: Cryptography and applications to security and privacy

Research topics (selection): Zero-knowledge proofs, commitment schemes, computation on encrypted data

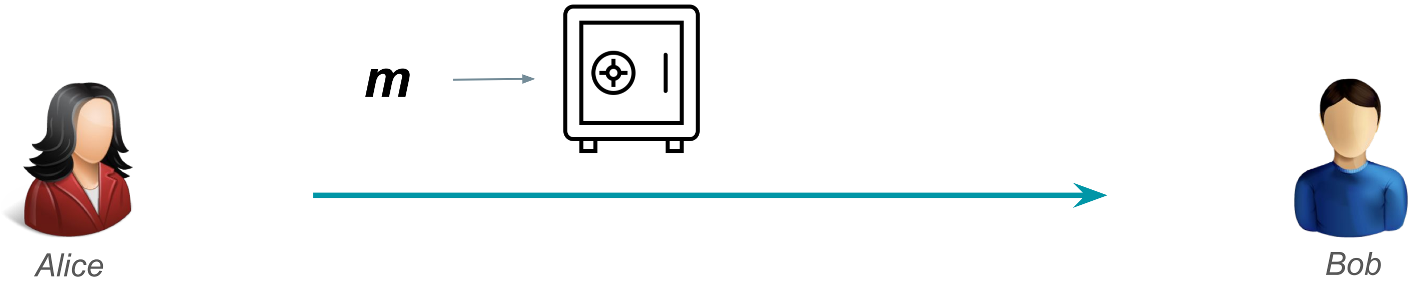
The problem of outsourced storage



How to get security while keeping O(1) storage and communication?

Commitments

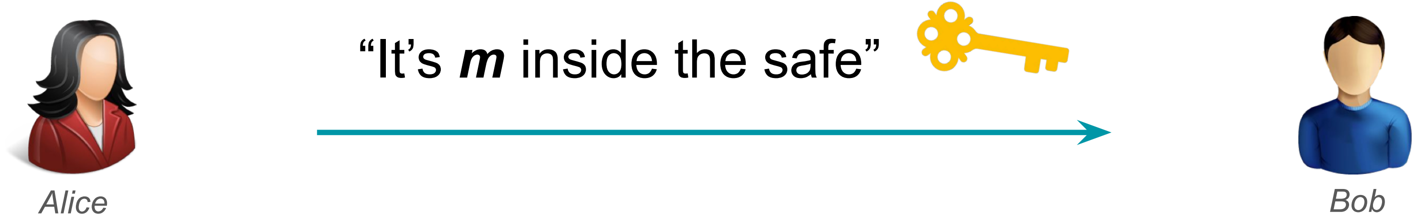
Commit phase

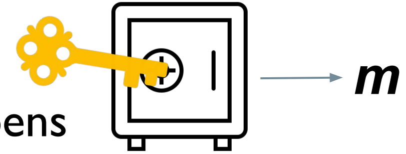


Dario Fiore IMDEA Software Institute, Madrid, Spain

Commitments

Opening phase





Security properties

- **Hiding:** Bob does not learn anything about ***m*** before Alice opens
- **Binding:** Alice cannot change her mind about ***m***, "hard" to open the same commitment to two distinct messages

Dario Fiore **IMDEA Software Institute, Madrid, Spain**

Commitment Schemes

Algorithms

- $\mathbf{Setup}(1^k) \rightarrow ck$
- $\mathbf{Com}(ck, x; r) \rightarrow C$
- $\mathbf{Open}(ck, x; r) \rightarrow \pi$
- $\mathbf{Ver}(ck, C, x, \pi) \rightarrow 0\ /1$ (reject/ accept)

Correctness: $\mathbf{Ver}\big(ck, \mathbf{Com}(ck, x; r), x, \mathbf{Open}(ck, x; r)\big) = 1$

Binding: for every probabilistic polynomial time (PPT) adversary $\boldsymbol{A}$ and any $ck \leftarrow \mathbf{Setup}(1^k)$ it holds

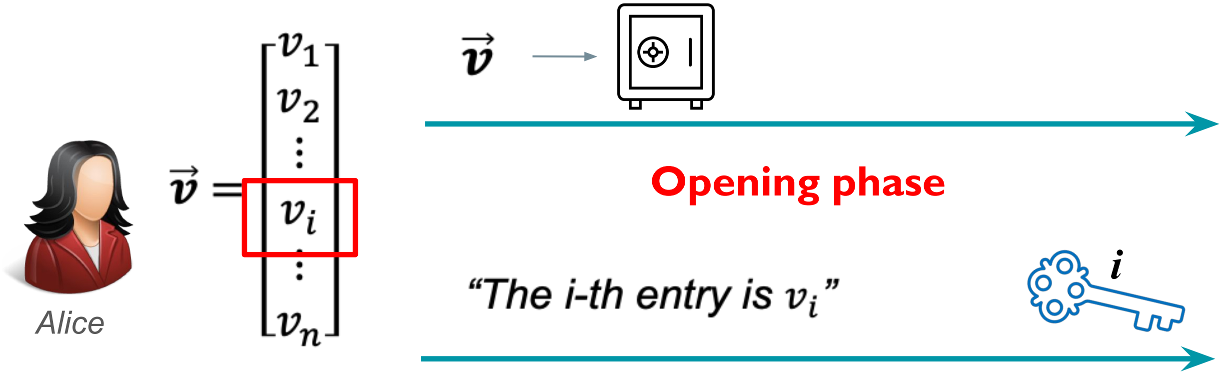
$$\Pr[x \neq x' \wedge \mathbf{Ver}(ck, C, x, \pi) = 1 \wedge \mathbf{Ver}(ck, C, x', \pi') = 1 \colon (C, x, \pi, x', \pi') \leftarrow \boldsymbol{A}(ck)] = \mathbf{negl}(k)$$

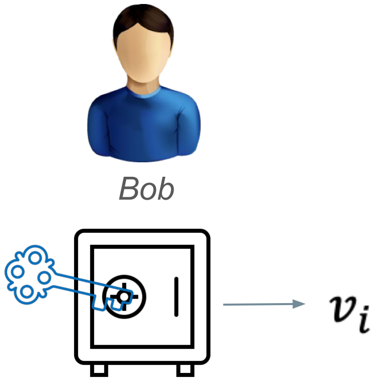
Hiding: for every PPT $\boldsymbol{A}$ and $\forall x \neq x'$: $\mathbf{Com}(ck, x; r) \approx \mathbf{Com}(ck, x'; r')$

Dario Fiore IMDEA Software Institute, Madrid, Spain

Vector Commitment Schemes [CF13]

[CF13] D. Catalano, D. Fiore. *Vector Commitments and their Applications*. PKC 2013





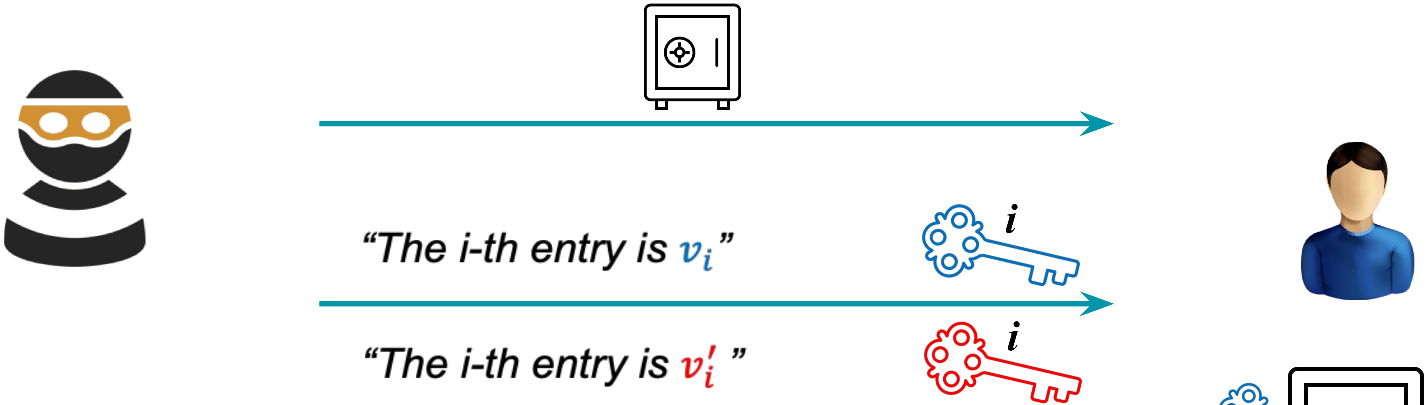
Basic idea: Commit to a vector and open single entries

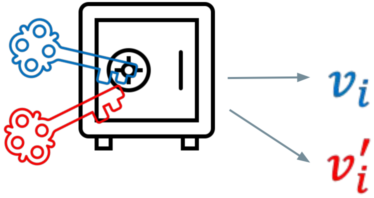
Key properties

- **Position binding:** can't open to two distinct values at the same position
- **Succinctness:** commitment and openings are short

Dario Fiore **IMDEA Software Institute, Madrid, Spain**

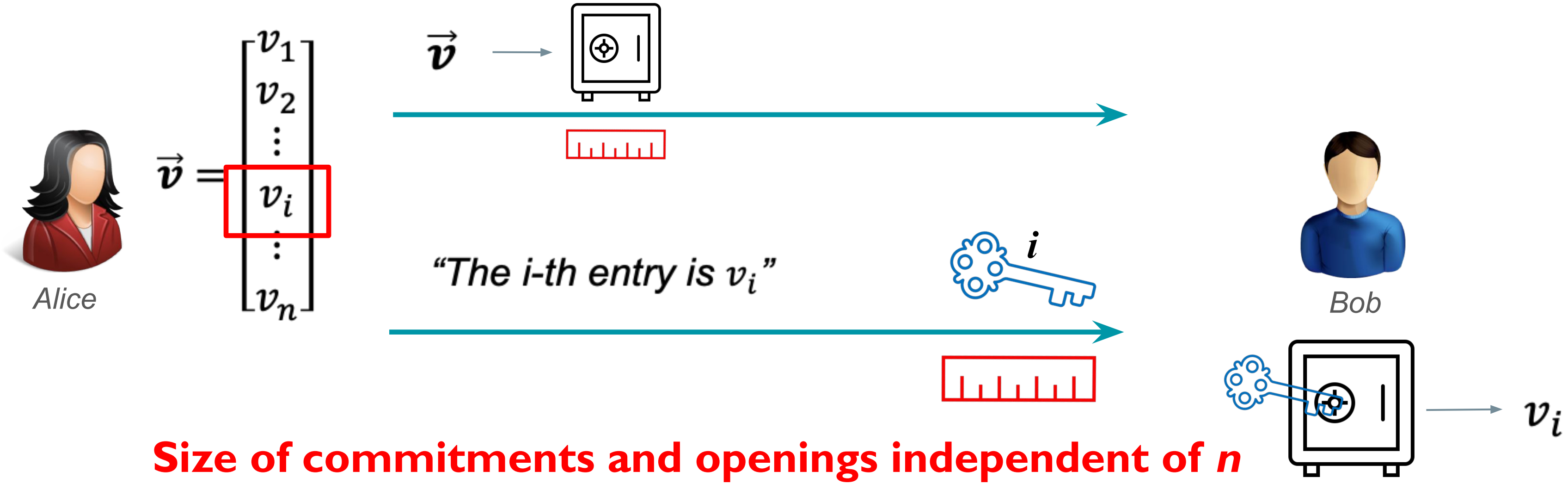
Position binding





It is hard to open the same commitment to
two different values at the same position

Succinctness



Size of commitments and openings independent of *n*

Note: non-succinct VCs, with O(n) commitments and O(1) openings, can be easily constructed from standard commitment schemes

Vector Commitment Schemes

Algorithms

- $\mathbf{Setup}(1^k, n) \to ck$
- $\mathbf{Com}(ck, \vec{v}) \to C$
- $\mathbf{Open}(ck, \vec{v}, i) \to \pi_i$
- $\mathbf{Ver}(ck, C, i, y, \pi_i) \to 0\ /1$ (*reject/ accept*)

Correctness: $\mathbf{Ver}\big(ck, \mathbf{Com}(ck, \vec{v}), i, v_i, \mathbf{Open}(ck, \vec{v}, i)\big) = 1$

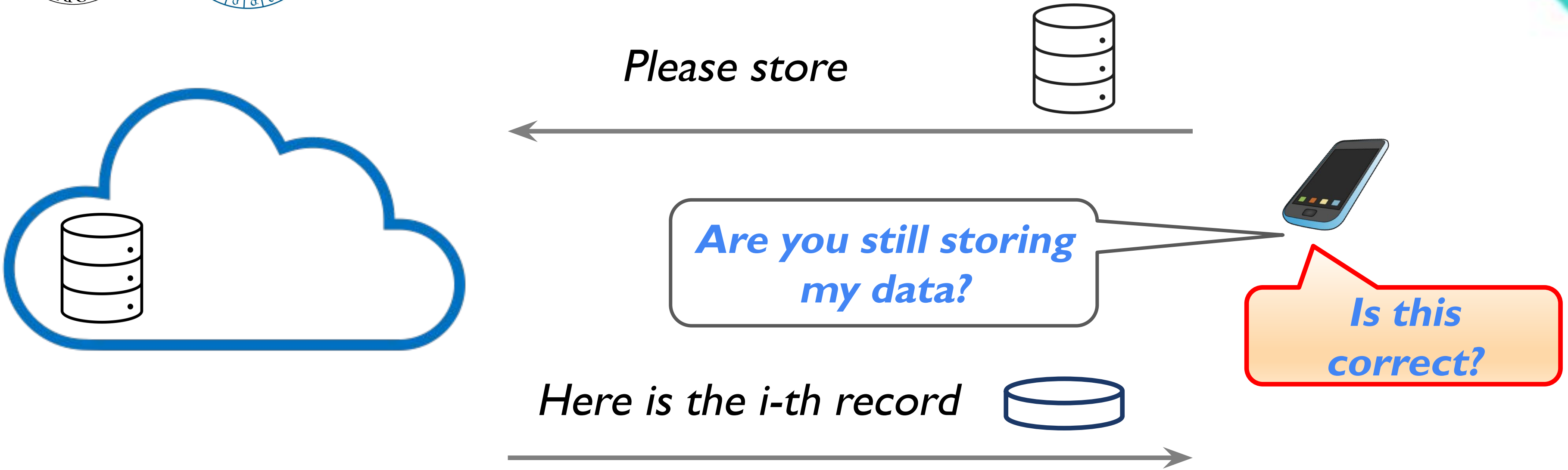
Position binding: for every probabilistic polynomial time (PPT) adversary ***A*** and any $ck \leftarrow \mathbf{Setup}(1^k, n)$ it holds

$$\Pr[y \neq y' \wedge \mathbf{Ver}(ck, C, i, y, \pi) = 1 \wedge \mathbf{Ver}(ck, C, i, y', \pi') = 1 : (C, i, y, \pi, y', \pi') \leftarrow \boldsymbol{A}(ck)] = \mathbf{negl}(k)$$

Succinctness: there is a fixed polynomial $p(k)$ s.t. $|C|, |\pi_i| \leq p(k)$

Dario Fiore IMDEA Software Institute, Madrid, Spain

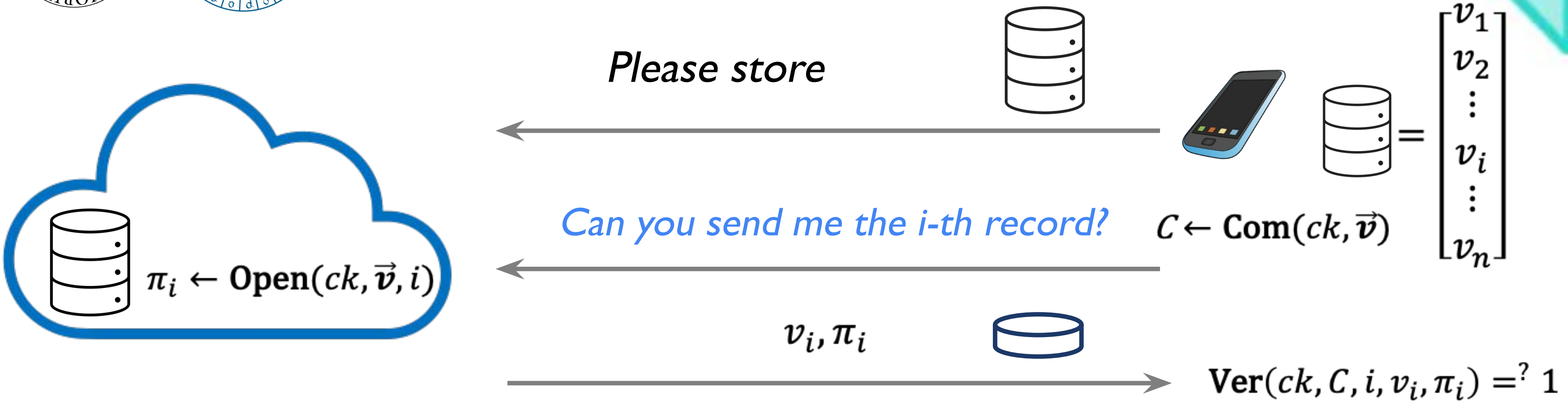
The problem of outsourced storage



How to get security while keeping O(1) storage and communication?

Dario Fiore IMDEA Software Institute, Madrid, Spain

VCs for outsourced storage



Storage: $|C| \leq p(k)$ **Communication:** $|\pi_i| \leq p(k)$ //independent of dataset

Security: relies on position binding.

If server cheats (i.e., sends $v_i' \neq v_i$ *with valid* π_i') we can break position binding.

Dario Fiore **IMDEA Software Institute, Madrid, Spain**

More applications of vector commitments

- Proofs of retrievability / proofs of space
- Stateless Blockchains
- Succinct Arguments
- Zero-knowledge sets
- Accumulators
- …

State of the art of VC constructions

[Merkle89] Merkle trees are vector commitments, albeit with O(log n)-size openings

[CFM08] preliminary notion "n-trapdoor mercurial commitments" (n-TMC≈VC w/more properties)

[LY10] first realization of n-TMC based on n-DHE assumption in bilinear groups

[CF13] first formalization of VC, constructions based on RSA or CDH in bilinear groups.

In the state of the art, **many realizations** from different assumptions such as

- Groups of unknown order (RSA)
- Groups with bilinear maps
- Lattices

A simple VC based on pairings [CF13]

Bilinear groups

$\boldsymbol{G}_1, \boldsymbol{G}_2, \boldsymbol{G}_T$ of prime order q (we use multiplicative notation)

Bilinear map $\boldsymbol{e}: \boldsymbol{G}_1 \times \boldsymbol{G}_2 \rightarrow \boldsymbol{G}_T$ that is

- efficiently computable
- non-degenerate: for all generators $g_1 \in \boldsymbol{G}_1, g_2 \in \boldsymbol{G}_2$: $e(g_1, g_2) \neq 1$
- bilinear $e(g_1^a, g_2^b) = e(g_1^b, g_2^a) = e(g_1, g_2)^{ab}$

CDH-based Vector Commitments

- $\mathsf{Setup}(1^k)$: sample random $\vec{\boldsymbol{\alpha}} = (\alpha_1, \cdots, \alpha_n), \vec{\boldsymbol{\beta}} = (\beta_1, \cdots, \beta_n)$ in $\mathbb{Z}_q$ and compute

$$ck = \begin{pmatrix} \{A_j = g_1^{\alpha_j}, B_j = g_2^{\beta_j}\}_{j=1,\dots,n} \\ \{H_{i,j} = g_1^{\alpha_i \beta_j}\}_{i,j=1,\cdots,n,i\neq j} \end{pmatrix} \in \boldsymbol{G}_1^{n^2} \times \boldsymbol{G}_2^n$$

- $\mathsf{Com}(ck, \vec{\boldsymbol{v}})$: $C = \prod_{j=1}^n A_j^{v_j}$
- $\mathsf{Open}(ck, \vec{\boldsymbol{v}}, i) \rightarrow \pi_i = \prod_{j=1, j\neq i}^n H_{j,i}^{v_j}$
- $\mathsf{Ver}(ck, C, i, y, \pi_i)$: accept iff $e(C, B_i) = e(\pi_i, g_2) e(A_i, B_i)^y$

Correctness: $e(C, B_i) = e\left(g_1^{\sum_{j=1}^n \alpha_j \cdot v_j}, g_2^{\beta_i}\right) = e(g_1, g_2)^{\sum_{j=1, j\neq i}^n \alpha_j \beta_i \cdot v_j + \alpha_i \beta_i \cdot v_i}$

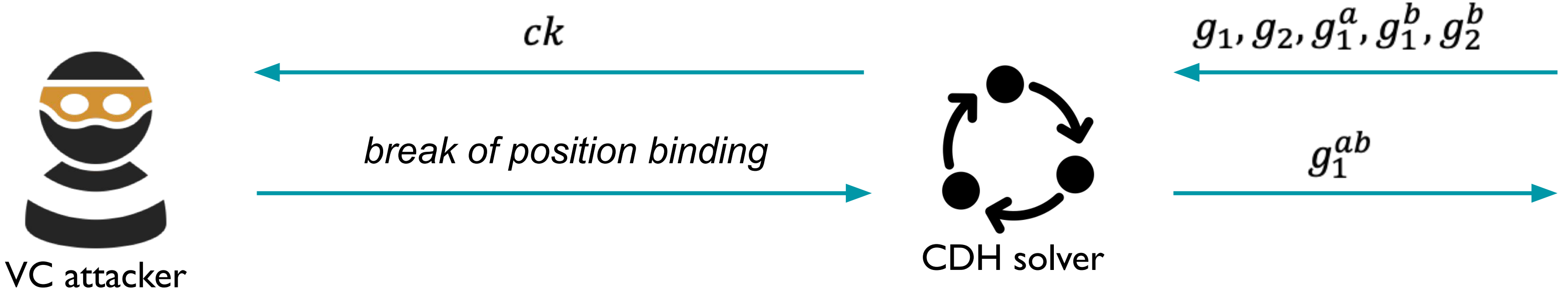
$$= e\left(g_1^{\sum_{j=1, j\neq i}^n \alpha_j \beta_i \cdot v_j}, g_2\right) e(g_1^{\alpha_i}, g_2^{\beta_i})^{v_i} = e(\pi_i, g_2)\, e(A_i, B_i)^{v_i}$$

Position binding under CDH

Computational Diffie-Hellman (CDH) Assumption: For every PPT adversary A

$$\Pr\left[A\left(g_1, g_2, g_1^a, g_1^b, g_2^b\right) = g_1^{ab} : a, b \leftarrow \mathbb{Z}_q\right] = negl(k)$$

Theorem: If the Computational Diffie-Hellman (CDH) Assumption holds, then the VC is position binding.



Dario Fiore IMDEA Software Institute, Madrid, Spain

Intuition of the security proof

- **Setup**(1^k): $A_j = g_1^{\alpha_j}, B_j = g_2^{\beta_j}\ : j = 1, \cdots, n\,; H_{i,j} = g_1^{\alpha_i \beta_j} : i, j = 1, \cdots, n, i \neq j$
- **Ver**(ck, C, i, y, π_i): accept iff $e(C, B_i) = e(\pi_i, g_2) e(A_i, B_i)^y$

Intuition: A breaking position binding w/prob. ϵ B solving CDH w/prob. ϵ/n.

$$A_j = \begin{cases} g_1^a : j = i \\ g_1^{\alpha_j} : j \neq i \end{cases}, B_j = \begin{cases} g_2^b : j = i \\ g_2^{\beta_j} : j \neq i \end{cases}, H_{j,k} = \begin{cases} (g_1^a)^{\beta_k} : j = i \\ (g_1^b)^{\alpha_j} : k = i \\ g_1^{\alpha_j \beta_k} : j, k \neq i \end{cases}$$

VC attacker

Commitment key

Position binding attack $(C, i, y, \pi_i, y', \pi_i')$

CDH solver

$g_1, g_2, g_1^a, g_1^b, g_2^b$

$$g_1^{ab} = g_1^{\alpha_i \beta_i} = \left(\frac{\pi_i}{\pi_i'}\right)^{1/(y'-y)}$$

$$e(C, B_i) = e(\pi_i, g_2) e(A_i, B_i)^y$$
$$e(C, B_i) = e(\pi_i', g_2) e(A_i, B_i)^{y'}$$
$$\Rightarrow e\left(\frac{\pi_i}{\pi_i'}, g_2\right) = e(A_i, B_i)^{y'-y} = e(g_1^{\alpha_i}, g_2^{\beta_i})^{y'-y} = e(g_1^{\alpha_i \beta_i}, g_2)^{y'-y}$$

Dario Fiore IMDEA Software Institute, Madrid, Spain

Conclusions

This lecture:

- The notion of vector commitments (succinctness & position binding are the key)
- Applications to outsourced storage (security & efficiency)
- A construction based on the CDH problem in bilinear groups

Active area of research (VCs with advanced properties):

- **Updatable VCs:** update Com(v) into Com(v') w/o recomputing [CF13]
- **Subvector openings:** constant-size opening to many positions [BBF19,LM19]

Dario Fiore IMDEA Software Institute, Madrid, Spain

- **Aggregation:** given compute [CFGKN20]

De Componendis Cifris

https:/www.decifris.it

Dario Fiore **IMDEA Software Institute**

References

[Merkle87] R. C. Merkle. *A Digital Signature Based on a Conventional Encryption Function.* CRYPTO 1987

[CFM08] D. Catalano, D. Fiore, and M. Messina. *Zero-knowledge sets with short proofs.* EUROCRYPT 2008

[LY10] B. Libert and M. Yung. *Concise Mercurial Vector Commitments and Independent Zero-Knowledge Sets with Short Proofs.* TCC 2010

[CF13] D. Catalano and D. Fiore. *Vector Commitments and Their Applications.* PKC 2013

[LRY16] B. Libert, S. C. Ramanna, and M. Yung. *Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions.* ICALP 2016

[BBF19] D. Boneh, B. Bünz, and B. Fisch. *Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains.* CRYPTO 2019

[LM19] R. W. F. Lai and G. Malavolta. *Subvector Commitments with Application to Succinct Arguments.* CRYPTO 2019

[CFGKN20] M. Campanelli, D. Fiore, N. Greco, D. Kolonelos, L. Nizzardo. *Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage.* ASIACRYPT 2020