Benoît Libert
Zama

December 11, 2024

Non-Malleable Subvector Commitments

Asiacrypt 2024 – Kolkata

ZAMA

Outline

Vector commitments: Properties, applications and prior work

Non-malleable (sub)vector commitments
- Motivation and definition of non-malleable SVC
- Simulation-sound subvector commitments (SS-SVC)

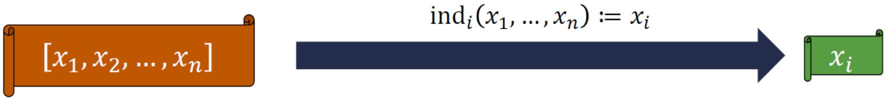
SS-SVC constructions
- Construction from Strong RSA: intuition and security
- Comparison with pairing-based SS-SVC

(Sub)Vector Commitments

Let a vector $(x_1, \dots, x_n) \in R^n$ over a ring R. A commitment

$$vcom = \textbf{Commit}(x_1, \dots, x_n)$$

can be **locally** opened to x_i for any $i \in [n]$



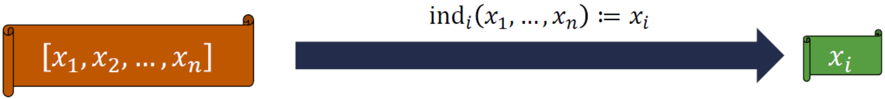
- $|vcom|$ and $|opening|$ should be $O(\lambda \cdot \mathrm{polylog}(n))$
- **Applications:**
  - ZK databases with short proofs (Catalano *et al.*, Eurocrypt'08; L.-Yung, TCC'10)
  - Verifiable data streaming [KSS+16], authenticated dictonaries [TXN20], cryptocurrencies [TAB+20], blockchain transactions [GRWZ20]
- SVC: $|opening| = O(\lambda \cdot \mathrm{polylog}(n, |S|))$ even if $\{x_i\}_{i \in S}$ are opened for $S \subseteq [n]$

(Sub)Vector Commitments

Let a vector $(x_1, \ldots, x_n) \in R^n$ over a ring R. A commitment

$$vcom = \textbf{Commit}(x_1, \ldots, x_n)$$

can be **locally** opened to x_i for any $i \in [n]$



- $|vcom|$ and $|opening|$ should be $O(\lambda \cdot \mathrm{polylog}(n))$
- **Applications:**
  - ZK databases with short proofs (Catalano *et al.*, Eurocrypt'08; L.-Yung, TCC'10)
  - Verifiable data streaming [KSS+16], authenticated dictonaries [TXN20], cryptocurrencies [TAB+20], blockchain transactions [GRWZ20]
- SVC: $|opening| = O(\lambda \cdot \mathrm{polylog}(n, |S|))$ even if $\{x_i\}_{i \in S}$ are opened for $S \subseteq [n]$

Prior Work on VCs (non-exhaustive)

- Folklore with $O(\log n)$-size openings via Merkle trees and CRHF
- Constructions with $O(1)$-size openings
  - From pairings and q-type assumptions (L.-Yung, TCC'10; Kate *et al.*, AC'10)
  - From CDH and hidden order groups (Catalano-Fiore, PKC'13; Boneh-Bünz-Fisch; Crypto'19)
  - From lattices (Peikert *et al.*, TCC'21; Albrecht *et al.*, Crypto'22; Wee-Wu, EC'23; …, …)
- Enhanced functionalities/security
  - Functional commitments for linear functions (L.-Ramanna-Yung, ICALP'16) and beyond (de Castro-Peikert, EC'23; Wee-Wu, EC'23)
  - Subvector openings (Lai-Malavolta; Boneh-Bünz-Fisch, Crypto'19)
  - Non-malleability (Rotem-Segev, TCC'21)

Non-Malleable Vector Commitments

- Adversary's local openings should not depend on honest local commitment openings (`Rotem-Segev, TCC'21`)
- **Applications:**
  - Blockchains: VC commits to state; local openings verified by validators
  - Simultaneous multi-round auctions: bidders bid for many items per round
- NM-VC can be built by composing (tag-based) equivocable commitments and a VC:

$$vcom = \mathsf{VC.Commit}\big(Com(\boldsymbol{m}[1], tag), \ldots, Com(\boldsymbol{m}[n], tag)\big),$$

where tag = one-time signature vk

(does not extend to the SVC setting)

Asiacrypt 2024

Non-Malleable Vector Commitments

- Adversary's local openings should not depend on honest local commitment openings (`Rotem-Segev, TCC'21`)
- **Applications:**
  - Blockchains: VC commits to state; local openings verified by validators
  - Simultaneous multi-round auctions: bidders bid for many items per round
- NM-VC can be built by composing (tag-based) equivocable commitments and a VC:

$$vcom = \mathbf{VC.Commit}(Com(\boldsymbol{m}[1], tag), \ldots, Com(\boldsymbol{m}[n], tag)),$$

where tag = one-time signature vk

(does not extend to the SVC setting)

Contributions: Non-Malleable Subvector Commitments

- Extension of the Rotem–Segev definition (TCC'21)
- Construction via an SVC-extension of simulation-sound trapdoor commitments (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04)
- Simulation-sound SVC from various assumptions
  - **Bilinear Diffie–Hellman** assumption: $O(n^2)$-size CRS; $O(n)$ exponentiations to commit
  - **Strong RSA** assumption: $O(1)$-size CRS; $O(n \cdot \log n)$ exponentiations to commit/open
  - **Strong Bilinear Diffie–Hellman** assumption: $O(n)$-size CRS; $O(n)$ exponentiations and $O(n \cdot \log^3 n)$ field operations to commit/open

NM-SVC Definition: Real experiment

$CRS \leftarrow \textbf{Setup}(\lambda)$
$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$
$(vcom, st) \leftarrow \textbf{Commit}_{crs}(\boldsymbol{m})$

$(CRS, vcom)$ →

← $\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t}, \; \pi_{S,i} \leftarrow \textbf{Open}_{crs}(vcom, S_i, st) \;\; \forall i \in [t]$ →

← $(\widehat{vcom}, \{\mathcal{J}_i \subseteq [n]\}_{i=1}^{s})$

Output

$$\left(\{S_i\}_{i=1}^{t}, \; \boldsymbol{m}, \; \{\mathcal{J}_i\}_{i=1}^{s}, \; (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s}, \; (\bot)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$$

with $\widehat{\boldsymbol{m}}_{\mathcal{J}_i} = (\bot)^{|\mathcal{J}_i|} \;\; \forall i \in [s]$ if $\widehat{vcom} = vcom$ or $\exists j \in [s] : \textbf{Verify}_{crs}(\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{vcom}, \widehat{\pi}_{\mathcal{J}_i}) = 0$

Asiacrypt 2024

NM-SVC Definition: Real experiment

$CRS \leftarrow \mathbf{Setup}(\lambda)$

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$(vcom, st) \leftarrow \mathbf{Commit}_{crs}(\boldsymbol{m})$

$(CRS, vcom)$ →

← $\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t},\ \pi_{S,i} \leftarrow \mathbf{Open}_{crs}(vcom, S_i, st) \quad \forall i \in [t]$ →

← $\left(\widehat{vcom},\ \{\mathcal{J}_i \subseteq [n]\}_{i=1}^{s}\right)$

$m_j, \pi_j \leftarrow \mathbf{Open}_{crs}(vcom, \{j\}, st) \quad \forall j \in [n] \setminus \bigcup_{i=1}^{t} S_i$ →

Output

$$\left(\{S_i\}_{i=1}^{t},\ \boldsymbol{m},\ \{\mathcal{J}_i\}_{i=1}^{s},\ (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s},\ (\bot)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$$

with $\widehat{\boldsymbol{m}}_{\mathcal{J}_i} = (\bot)^{|\mathcal{J}_i|} \quad \forall i \in [s]$ if $\widehat{vcom} = vcom$ or $\exists j \in [s] : \mathbf{Verify}_{crs}(\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{vcom}, \widehat{\pi}_{\mathcal{J}_i}) = 0$

NM-SVC Definition: Real experiment

$CRS \leftarrow \textbf{Setup}(\lambda)$

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$(vcom, st) \leftarrow \textbf{Commit}_{crs}(\boldsymbol{m})$

$(CRS, vcom)$ →

← $\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t},\ \pi_{S,i} \leftarrow \textbf{Open}_{crs}(vcom, S_i, st) \quad \forall i \in [t]$ →

← $\left(\widehat{vcom},\ \{\mathcal{J}_i \subseteq [n]\}_{i=1}^{s}\right)$

$m_j, \pi_j \leftarrow \textbf{Open}_{crs}(vcom, \{j\}, st) \quad \forall j \in [n] \setminus \bigcup_{i=1}^{t} S_i$ →

← $\{\widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{\pi}_{\mathcal{J}_i}\}_{i=1}^{s}$

Output

$$\left(\{S_i\}_{i=1}^{t},\ \boldsymbol{m},\ \{\mathcal{J}_i\}_{i=1}^{s},\ (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s},\ (\bot)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$$

with $\widehat{\boldsymbol{m}}_{\mathcal{J}_i} = (\bot)^{|\mathcal{J}_i|} \quad \forall i \in [s]$ if $\widehat{vcom} = vcom$ or $\exists j \in [s] : \textbf{Verify}_{crs}(\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{vcom}, \widehat{\pi}_{\mathcal{J}_i}) = 0$

NM-SVC Definition: Real experiment

$CRS \leftarrow \mathbf{Setup}(\lambda)$
$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$
$(vcom, st) \leftarrow \mathbf{Commit}_{crs}(\boldsymbol{m})$

$(CRS, vcom)$ →

← $\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t},\ \pi_{S,i} \leftarrow \mathbf{Open}_{crs}(vcom, S_i, st) \quad \forall i \in [t]$ →

← $\left(\widehat{vcom},\ \{\mathcal{J}_i \subseteq [n]\}_{i=1}^{s}\right)$

$m_j, \pi_j \leftarrow \mathbf{Open}_{crs}(vcom, \{j\}, st) \quad \forall j \in [n] \setminus \bigcup_{i=1}^{t} S_i$ →

← $\{\widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{\pi}_{\mathcal{J}_i}\}_{i=1}^{s}$

Output

$$\left(\{S_i\}_{i=1}^{t},\ \boldsymbol{m},\ \{\mathcal{J}_i\}_{i=1}^{s},\ (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s},\ (\perp)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$$

with $\widehat{\boldsymbol{m}}_{\mathcal{J}_i} = (\perp)^{|\mathcal{J}_i|} \quad \forall i \in [s]$ if $\widehat{vcom} = vcom$ or $\exists j \in [s] : \mathbf{Verify}_{crs}(\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{vcom}, \widehat{\pi}_{\mathcal{J}_i}) = 0$

NM–SVC Definition: Real experiment

$CRS \leftarrow \textbf{Setup}(\lambda)$
$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$
$(vcom, st) \leftarrow \textbf{Commit}_{crs}(\boldsymbol{m})$

$(CRS, vcom)$ →

← $\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t},\ \pi_{S,i} \leftarrow \textbf{Open}_{crs}(vcom, S_i, st) \quad \forall i \in [t]$ →

← $\left(\widehat{vcom},\ \{\mathcal{J}_i \subseteq [n]\}_{i=1}^{s}\right)$

$m_j, \pi_j \leftarrow \textbf{Open}_{crs}(vcom, \{j\}, st) \quad \forall j \in [n] \setminus \bigcup_{i=1}^{t} S_i$ →

← $\{\widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{\pi}_{\mathcal{J}_i}\}_{i=1}^{s}$

Output

$$\left(\{S_i\}_{i=1}^{t},\ \boldsymbol{m},\ \{\mathcal{J}_i\}_{i=1}^{s},\ (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s},\ (\perp)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$$

with $\widehat{\boldsymbol{m}}_{\mathcal{J}_i} = (\perp)^{|\mathcal{J}_i|} \quad \forall i \in [s]$ if $\widehat{vcom} = vcom$ or $\exists j \in [s] : \textbf{Verify}_{crs}(\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}, \widehat{vcom}, \widehat{\pi}_{\mathcal{J}_i}) = 0$

NM-SVC Definition: Ideal experiment

For any PPT $\mathcal{A}$ in **Real**, there is a PPT simulator $\mathcal{S}$ in **Ideal** s.t., for any valid $\mathcal{D}$, **Real** and **Ideal** have indistinguishable outputs

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$\{S_i \subseteq [n]\}_{i=1}^{t}$

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t}$

$\mathcal{S}$

NM-SVC Definition: Ideal experiment

For any PPT $\mathcal{A}$ in **Real**, there is a PPT simulator $\mathcal{S}$ in **Ideal** s.t., for any valid $\mathcal{D}$, **Real** and **Ideal** have indistinguishable outputs

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$\{S_i \subseteq [n]\}_{i=1}^{t}$ ←

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t}$ →

$\{\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}\}_{i=1}^{s}$ ←

$\mathcal{S}$

Output $\left(\{S_i\}_{i=1}^{t}, \boldsymbol{m}, \{\mathcal{J}_i\}_{i=1}^{s}, (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s}, (\perp)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$

- $\mathcal{D}$ should support efficient conditional re-sampling:

  For any $\boldsymbol{m} \sim \mathcal{D}$, any $S \subseteq [n]$, the following distribution is efficiently samplable

  $$\mathcal{D} \mid (\forall i \in S : \boldsymbol{m}'[i] = \boldsymbol{m}[i])$$

- Definition does not capture re-usability (Damgård–Groth , STOC '03)

NM-SVC Definition: Ideal experiment

For any PPT $\mathcal{A}$ in **Real**, there is a PPT simulator $\mathcal{S}$ in **Ideal** s.t., for any valid $\mathcal{D}$, **Real** and **Ideal** have indistinguishable outputs

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$\{S_i \subseteq [n]\}_{i=1}^{t}$ ←

$\{\boldsymbol{m}_{S_i}\}_{i=1}^{t}$ →

$\{\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}\}_{i=1}^{s}$ ←

$\mathcal{S}$

Output $\left(\{S_i\}_{i=1}^{t}, \boldsymbol{m}, \{\mathcal{J}_i\}_{i=1}^{s}, (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s}, (\perp)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$

- $\mathcal{D}$ should support efficient conditional re-sampling:

  For any $\boldsymbol{m} \sim \mathcal{D}$, any $S \subseteq [n]$, the following distribution is efficiently samplable

$$\mathcal{D} \mid (\forall i \in S : \boldsymbol{m}'[i] = \boldsymbol{m}[i])$$

- Definition does not capture re-usability (Damgård-Groth, STOC'03)

NM-SVC Definition: Ideal experiment

For any PPT $\mathcal{A}$ in **Real**, there is a PPT simulator $\mathcal{S}$ in **Ideal** s.t., for any valid $\mathcal{D}$, **Real** and **Ideal** have indistinguishable outputs

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$\longleftarrow \{S_i \subseteq [n]\}_{i=1}^{t}$

$\longrightarrow \{\boldsymbol{m}_{S_i}\}_{i=1}^{t}$

$\longleftarrow \{\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}\}_{i=1}^{s}$

$\mathcal{S}$

Output $\left(\{S_i\}_{i=1}^{t}, \boldsymbol{m}, \{\mathcal{J}_i\}_{i=1}^{s}, (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s}, (\bot)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$

- $\mathcal{D}$ should support efficient conditional re-sampling:

  For any $\boldsymbol{m} \sim \mathcal{D}$, any $S \subseteq [n]$, the following distribution is efficiently samplable

$$\mathcal{D} \mid (\forall i \in S : \boldsymbol{m}'[i] = \boldsymbol{m}[i])$$

- Definition does not capture re-usability (`Damgård-Groth, STOC'03`)

NM-SVC Definition: Ideal experiment

For any PPT $\mathcal{A}$ in **Real**, there is a PPT simulator $\mathcal{S}$ in **Ideal** s.t., for any valid $\mathcal{D}$, **Real** and **Ideal** have indistinguishable outputs

$\boldsymbol{m} = (m_1, \ldots, m_n) \hookleftarrow \mathcal{D}$

$\mathcal{S}$

$\leftarrow \{S_i \subseteq [n]\}_{i=1}^{t}$

$\rightarrow \{\boldsymbol{m}_{S_i}\}_{i=1}^{t}$

$\leftarrow \{\mathcal{J}_i, \widehat{\boldsymbol{m}}_{\mathcal{J}_i}\}_{i=1}^{s}$

Output $\left(\{S_i\}_{i=1}^{t}, \boldsymbol{m}, \{\mathcal{J}_i\}_{i=1}^{s}, (\widehat{\boldsymbol{m}}_{\mathcal{J}_i})_{i=1}^{s}, (\perp)^{n-|\bigcup_{i=1}^{s}\mathcal{J}_i|}\right)$

- $\mathcal{D}$ should support efficient conditional re-sampling:

  For any $\boldsymbol{m} \sim \mathcal{D}$, any $S \subseteq [n]$, the following distribution is efficiently samplable

  $$\mathcal{D} \mid (\forall i \in S : \boldsymbol{m}'[i] = \boldsymbol{m}[i])$$

- Definition does not capture re-usability (`Damgård-Groth, STOC'03`)

Simulation-Sound (Trapdoor) SVC

Syntax extends SSTCs (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

- **Setup**(λ, n) : outputs crs and a trapdoor tk.
- **Commit**$(tag, \boldsymbol{m} \in R^n)$: outputs a commitment $vcom$ and a state $st = (\boldsymbol{m}, r)$.
- **Open**$(tag, \boldsymbol{m}, S \subseteq [n], st)$: outputs subvector $\boldsymbol{m}_S$ and a short π_S
- **Verify**$(tag, vcom, S \subseteq [n], \boldsymbol{m}_S, st)$: returns 0 or 1

- **FakeCom**(tag, tk) : outputs a fake commitment $\widetilde{vcom}$ and a state st.
- **FakeOpen**$(tag, tk, \boldsymbol{m}_S, S \subseteq [n], st)$: outputs $\boldsymbol{m}_S$ and a short π_S

Simulation–Sound (Trapdoor) SVC

Syntax extends SSTCs (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

- **Setup**(λ, n) : outputs crs and a trapdoor tk.
- **Commit**$(tag, \boldsymbol{m} \in R^n)$: outputs a commitment $vcom$ and a state $st = (\boldsymbol{m}, r)$.
- **Open**$(tag, \boldsymbol{m}, S \subseteq [n], st)$: outputs subvector $\boldsymbol{m}_S$ and a short π_S
- **Verify**$(tag, vcom, S \subseteq [n], \boldsymbol{m}_S, st)$: returns 0 or 1

- **FakeCom**(tag, tk) : outputs a fake commitment $\widetilde{vcom}$ and a state st.
- **FakeOpen**$(tag, tk, \boldsymbol{m}_S, S \subseteq [n], st)$: outputs $\boldsymbol{m}_S$ and a short π_S

Simulation-Sound (Trapdoor) SVC

Simulation-Sound binding (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

$(CRS, TK) \leftarrow \mathbf{Setup}(\lambda)$

CRS

tag_i

$\widetilde{vcom_i} \leftarrow \mathbf{FakeCom}(tag_i, TK)$

Adversary wins if:

- $tag^* \notin \{tag_i\}_{i \in [Q]} \quad \wedge \quad \mathbf{Verify}(crs, tag^*, S_b, \boldsymbol{m}_{S_b}, vcom^*, \pi_{S,b}) = 1 \quad \forall b \in \{1, 2\}$
- $\exists i \in S_1 \cap S_2 \;\; \text{s.t.} \;\; \boldsymbol{m}_{S_1}[i] \neq \boldsymbol{m}_{S_2}[i]$

Simulation–Sound (Trapdoor) SVC

Simulation–Sound binding (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

$(CRS, TK) \leftarrow \textbf{Setup}(\lambda)$

CRS →

⋮

← tag_i

$\widetilde{vcom}_i \leftarrow \textbf{FakeCom}(tag_i, TK)$ →

← $tag_i,\ S_i \subseteq [n],\ \mathbf{m}_{S_i}$

$\tilde{\pi}_{S_i} \leftarrow \textbf{FakeOpen}(tag_i, TK, S_i, \mathbf{m}_{S_i})$ →

⋮

← $tag^*,\ vcom^*,\ S_1,\ S_2,\ \mathbf{m}_{S_1},\ \mathbf{m}_{S_2},\ \pi_{S,1},\ \pi_{S,2}$

Adversary wins if:

- $tag^* \notin \{tag_i\}_{i \in [Q]} \quad \wedge \quad \textbf{Verify}(crs, tag^*, S_b, \mathbf{m}_{S_b}, vcom^*, \pi_{S,b}) = 1 \quad \forall b \in \{1,2\}$
- $\exists i \in S_1 \cap S_2 \text{ s.t. } \mathbf{m}_{S_1}[i] \neq \mathbf{m}_{S_2}[i]$

Simulation-Sound (Trapdoor) SVC

Simulation-Sound binding (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

$(CRS, TK) \leftarrow \mathbf{Setup}(\lambda)$

CRS →

⋮

← tag_i

$\widetilde{vcom}_i \leftarrow \mathbf{FakeCom}(tag_i, TK)$ →

← $tag_i,\ S_i \subseteq [n],\ \mathbf{m}_{S_i}$

$\tilde{\pi}_{S_i} \leftarrow \mathbf{FakeOpen}(tag_i, TK, S_i, \mathbf{m}_{S_i})$ →

⋮

← $tag^\star,\ vcom^\star,\ S_1,\ S_2,\ \mathbf{m}_{S_1},\ \mathbf{m}_{S_2},\ \pi_{S,1},\ \pi_{S,2}$

Adversary wins if:

- $tag^\star \notin \{tag_i\}_{i\in[Q]} \quad \wedge \quad \mathbf{Verify}(crs, tag^\star, S_b, \mathbf{m}_{S_b}, vcom^\star, \pi_{S,b}) = 1 \quad \forall b \in \{1,2\}$
- $\exists i \in S_1 \cap S_2 \text{ s.t. } \mathbf{m}_{S_1}[i] \neq \mathbf{m}_{S_2}[i]$

Simulation–Sound (Trapdoor) SVC

Simulation–Sound binding (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

$(CRS, TK) \leftarrow \textbf{Setup}(\lambda)$

CRS →

⋮

← tag_i

$\widetilde{vcom}_i \leftarrow \textbf{FakeCom}(tag_i, TK)$ →

← $tag_i,\ S_i \subseteq [n],\ \mathbf{m}_{S_i}$

$\widetilde{\pi}_{S_i} \leftarrow \textbf{FakeOpen}(tag_i, TK, S_i, \mathbf{m}_{S_i})$ →

⋮

← $tag^\star,\ vcom^\star,\ S_1,\ S_2,\ \mathbf{m}_{S_1},\ \mathbf{m}_{S_2},\ \pi_{S,1},\ \pi_{S,2}$

Adversary wins if:

- $tag^\star \notin \{tag_i\}_{i\in[Q]} \quad \wedge \quad \textbf{Verify}(crs, tag^\star, S_b, \boldsymbol{m}_{S_b}, vcom^\star, \pi_{S,b}) = 1 \quad \forall b \in \{1,2\}$
- $\exists i \in S_1 \cap S_2 \ \text{ s.t. } \ \boldsymbol{m}_{S_1}[i] \neq \boldsymbol{m}_{S_2}[i]$

Simulation–Sound (Trapdoor) SVC

Simulation–Sound binding (Garay *et al.*, Eurocrypt'03; MacKenzie-Yang, Eurocrypt'04):

$(CRS, TK) \leftarrow \mathbf{Setup}(\lambda)$

CRS →

⋮

← tag_i

$\widetilde{vcom}_i \leftarrow \mathbf{FakeCom}(tag_i, TK)$ →

← $tag_i,\ S_i \subseteq [n],\ \mathbf{m}_{S_i}$

$\tilde{\pi}_{S_i} \leftarrow \mathbf{FakeOpen}(tag_i, TK, S_i, \mathbf{m}_{S_i})$ →

⋮

← $tag^\star,\ vcom^\star,\ S_1,\ S_2,\ \mathbf{m}_{S_1},\ \mathbf{m}_{S_2},\ \pi_{S,1},\ \pi_{S,2}$

Adversary wins if:

- $tag^\star \notin \{tag_i\}_{i\in[Q]} \quad \wedge \quad \mathbf{Verify}\big(crs, tag^\star, S_b, \boldsymbol{m}_{S_b}, vcom^\star, \pi_{S,b}\big) = 1 \quad \forall b \in \{1,2\}$
- $\exists i \in S_1 \cap S_2$ s.t. $\boldsymbol{m}_{S_1}[i] \neq \boldsymbol{m}_{S_2}[i]$

NM-SVC from Simulation-Sound SVC

Strong one-time signature (+ UOWHF)

+

Simulation-sound subvector commitment

$\Longrightarrow$ NM-SVC

- SS-SVC tag is a one-time signature verification key; commitments are signed
- Extends construction of (re-usable) NM commitments from SS trapdoor commitments (MacKenzie-Yang, Eurocrypt'04)

SS-SVC from 3 Assumptions

The Bilinear Diffie-Hellman (BDH) problem

In pairing-frienly groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p: given

$$\left(g,\ g^a,\ g^b,\ g^c\right) \in \mathbb{G}^4, \qquad \left(\hat{g},\ \hat{g}^a,\ \hat{g}^b,\ \hat{g}^c\right) \in \hat{\mathbb{G}}^4$$

with $a, b, c \xleftarrow{R} \mathbb{Z}_p$, compute $e(g, \hat{g})^{abc}$

The Strong Bilinear Diffie-Hellman (q-SBDH) problem

In pairing-friendly groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$, given

$$\left(g,\ g^\alpha,\ \ldots,\ g^{(\alpha^q)}\right), \quad \left(\hat{g},\ \hat{g}^\alpha,\ \ldots,\ \hat{g}^{(\alpha^q)}\right)$$

with $\alpha \xleftarrow{R} \mathbb{Z}_p$, find a pair $\left(c,\ e(g, \hat{g})^{1/(\alpha+c)}\right) \in \mathbb{Z}_p \times \hat{\mathbb{G}}_T$

The Strong RSA problem

Given a safe-prime product $N = pq$ and $y \xleftarrow{R} \mathbb{Z}_N^*$, find $e > 1$ and $x \in \mathbb{Z}_N^*$ s.t.

$$y = x^e \bmod N$$

SS-SVC from Strong RSA

- Builds on (`Lai-Malavolta, Crypto'19; Catalano-Fiore, PKC'13`)
- CRS contains a safe-prime product $N = pq$ and a generator $g_0 \in \mathbb{QR}_N$;
- Uses public primes $\{e_i\}_{i=1}^n$ longer than committed $m_i \in \{0,1\}^k$
- Commits to $(m_1, \dots, m_n)$ by setting $g_i = g_0^{\prod_{j \neq i} e_j}$ for $i \in [n]$ and computing

$$vcom = \prod_{i=1}^{n} g_i^{m_i}$$

- **Idea of LM19:** Since

$$vcom \,/ \prod_{i \in S} g_i^{m_i} = g_0^{\sum_{i \in [n] \setminus S} m_i \cdot \prod_{j \neq i} e_j}$$

committer can open $S \subseteq [n]$ via a root $\pi_S = \left(vcom \,/ \prod_{i \in S} g_i^{m_i}\right)^{1 / \prod_{i \in S} e_i}$

SS-SVC from Strong RSA

- **Randomize the commitment:** Add an extra $g = g_0^{\prod_{i \in [n]} e_i}$ and commit to $(m_1, \ldots, m_n)$ via

$$vcom = g^r \cdot \prod_{i=1}^{n} g_i^{m_i}$$

with $r \xleftarrow{R} \mathbb{Z}_{(N-1)/4}$ (still binding although $\log_{g_i}(g) = e_i$ is public)

- **Handle equivocation queries** on $tag \neq tag^\star$
  - Knowing $g_i^{1/e_i} \bmod N$ for all $i \in [n]$ allows equivocating m_i
  - Equivocating on **non-adaptively chosen** $tag_j \neq tag^\star$ is sufficient
  - Primes $\{e_i\}_{i=1}^n$ can be derived from collision-resistant hash $\{e_i = H(tag, i)\}_{i=1}^n$ (cf. `Gennaro; Crypto'04`)

SS-SVC from Strong RSA

- **Commit**$(tag, \boldsymbol{m} = (m_1, \ldots, m_n))$: Generate $\{e_i = H(tag, i)\}_{i=1}^{n}$
  - Set $g = g_0^{\prod_{j\in[n]} e_j} \bmod N$ and $g_i = g_0^{\prod_{j\neq i} e_j} \bmod N$ for $i \in [n]$
  - Compute

$$vcom = g^r \cdot \prod_{i=1}^{n} g_i^{m_i} \bmod N$$

- **Open**$(tag, S \subseteq [n], st = (\boldsymbol{m}, r))$: Set $e_S \triangleq \prod_{i\in S} e_i$ and output

$$\pi_S = \left(vcom \,/\, \prod_{i\in S} g_i^{m_i}\right)^{1/e_S} \bmod N$$

- **Verify**$(tag, S, \boldsymbol{m}_S, C)$: Accept iff $vcom = \pi_S^{e_S} \cdot \prod_{i\in S} g_i^{m_i} \bmod N$

Remark:

- **Commit** takes $O(n \cdot \log n)$ exponentiations using (`Boneh-Bünz-Fisch; Crypto'19`)

SS-SVC from Strong RSA: Security

Theorem

The scheme is (non-adaptive) **simulation-sound binding** if the Strong RSA assumption holds and H is collision-resitant

- Reduction $\mathcal{B}$ breaks H or a Strong RSA instance $(N = pq,\ y \in \mathbb{Z}_N^*)$
- Adversary $\mathcal{A}$ declares equivocable $\{tag_i\}_{i=1}^{Q}$; $\mathcal{B}$ computes $\{e_{i,j} = H(tag_i, j)\}_{i\in[Q],j\in[n]}$ and

$$g_0 = y^{2\cdot\prod_{i=1}^{Q}\prod_{j=1}^{n} e_{i,j}} \mod N$$

$\Rightarrow$ For any $e_{S,i} = \prod_{k\in S} e_{i,k}$, $\mathcal{B}$ can use an $e_{S,i}$-th root of g_0 to equivocate on tag_i

- If $\mathcal{A}$ succeeds for $tag^\star \notin \{tag_i\}_{i=1}^{Q}$, $\mathcal{B}$ obtains either a collision on H or

$$g_0^{1/e_{tag^\star}} \mod N$$

with $e_{tag^\star} = H(tag^\star, i^\star)$ for some $i^\star \in [n]$ such that $e_{tag^\star} \notin \bigcup_{i\in[Q],j\in[n]} e_{i,j}$

SS-SVC from Strong RSA: Security

Theorem

The scheme is (non-adaptive) **simulation-sound binding** if the Strong RSA assumption holds and H is collision-resitant

- Reduction $\mathcal{B}$ breaks H or a Strong RSA instance $(N = pq,\ y \in \mathbb{Z}_N^*)$
- Adversary $\mathcal{A}$ declares equivocable $\{tag_i\}_{i=1}^{Q}$; $\mathcal{B}$ computes $\{e_{i,j} = H(tag_i, j)\}_{i\in[Q],j\in[n]}$ and

$$g_0 = y^{2\cdot\prod_{i=1}^{Q}\prod_{j=1}^{n} e_{i,j}} \bmod N$$

$\Rightarrow$ For any $e_{S,i} = \prod_{k\in S} e_{i,k}$, $\mathcal{B}$ can use an $e_{S,i}$-th root of g_0 to equivocate on tag_i

- If $\mathcal{A}$ succeeds for $tag^\star \notin \{tag_i\}_{i=1}^{Q}$, $\mathcal{B}$ obtains either a collision on H or

$$g_0^{1/e_{tag^\star}} \bmod N$$

with $e_{tag^\star} = H(tag^\star, i^\star)$ for some $i^\star \in [n]$ such that $e_{tag^\star} \notin \bigcup_{i\in[Q],j\in[n]} e_{i,j}$

Asiacrypt 2024

SS-SVC from Strong RSA: Security

Theorem

The scheme is (non-adaptive) **simulation-sound binding** if the Strong RSA assumption holds and H is collision-resitant

- Reduction $\mathcal{B}$ breaks H or a Strong RSA instance $(N = pq,\ y \in \mathbb{Z}_N^*)$
- Adversary $\mathcal{A}$ declares equivocable $\{tag_i\}_{i=1}^{Q}$; $\mathcal{B}$ computes $\{e_{i,j} = H(tag_i, j)\}_{i\in[Q],j\in[n]}$ and

$$g_0 = y^{2\cdot\prod_{i=1}^{Q}\prod_{j=1}^{n} e_{i,j}} \mod N$$

$\Rightarrow$ For any $e_{S,i} = \prod_{k\in S} e_{i,k}$, $\mathcal{B}$ can use an $e_{S,i}$-th root of g_0 to equivocate on tag_i

- If $\mathcal{A}$ succeeds for $tag^\star \notin \{tag_i\}_{i=1}^{Q}$, $\mathcal{B}$ obtains either a collision on H or

$$g_0^{1/e_{tag^\star}} \mod N$$

with $e_{tag^\star} = H(tag^\star, i^\star)$ for some $i^\star \in [n]$ such that $e_{tag^\star} \notin \bigcup_{i\in[Q],j\in[n]} e_{i,j}$

Pairing-Based SS-SVC and Comparisons

Pairing-based constructions:

- From q-BSDH (pairing-based analogue of Strong-RSA-based scheme)
- From BDH: via opening aggregation (Gorbunov *et al.*; CCS'20; Catalano-Fiore, PKC'13);

  Equivocates using Waters signatures on tags (Eurocrypt'05)

Assumptions	CRS size	Opening size	Commit/Open cost	Verifier cost
Strong RSA	$O(1) \times \lvert\mathbb{Z}_N^*\rvert$	$1 \times \lvert\mathbb{Z}_N^*\rvert$	$O(n \cdot \log n)$ $\exp_{\mathbb{Z}_N^*}$	$O(n \cdot \log n)$ $\exp_{\mathbb{Z}_N^*}$
q-BSDH	$O(n) \times \lvert\hat{\mathbb{G}}\rvert$	$1 \times \lvert\mathbb{G}\rvert$	$O(n)$ $\exp_{\mathbb{G}}$ + $O(n \cdot \log^3 n)$ $\text{mult}_{\mathbb{Z}_p}$	$O(\lvert S\rvert)$ $\exp_{\hat{\mathbb{G}}}$ + $O(n \cdot \log^3 n)$ $\text{mult}_{\mathbb{Z}_p}$ + 2P
BDH	$O(n^2) \times \lvert\hat{\mathbb{G}}\rvert$	$2 \times \lvert\mathbb{G}\rvert$	$O(n)$ $\exp_{\mathbb{G}}$ / $O(n \cdot \lvert S\rvert)$ $\exp_{\mathbb{G}}$	$O(\lvert S\rvert)$ $\exp_{\hat{\mathbb{G}}_T}$ + 3P

Figure: Comparison for dimension-n vectors and suvectors of size $|S|$

Summary

- First constructions of NM-SVC (with re-usability)
- Direct constructions of SS-SVC from falsifiable assumptions:
  - BDH: linear-time commit/open but $O(n^2)$-size CRS
  - Strong RSA: $O(1)$-size CRS, but $O(n \log n)$-time commit/open
  - q-BSDH: $O(n)$-size CRS, $O(n \log^3 n)$-time commit/open (only $O(n)$ exponentiations)
- **Open problems:**
  - $O(n)$-size CRS, $O(n)$-time commit/open
  - Post-quantum constructions

Questions?

Contact and Links

benoit.libert@zama.ai

zama.ai

Github

Community

ZAMA