上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

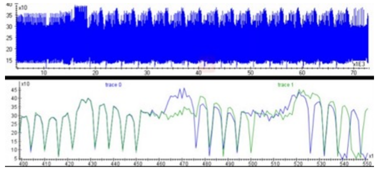
More Efficient Public-Key Cryptography with Leakage and Tamper Resilience

Shuai Han, Shengli Liu, Dawu Gu

Shanghai Jiao Tong University

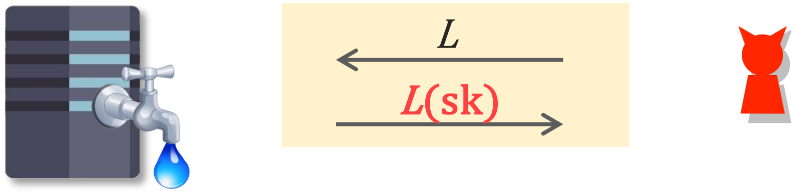
PKC 2024, Sydney, Australia

Key Leakage



Side-Channel Attacks
- Power
- Time
- Sound
- …

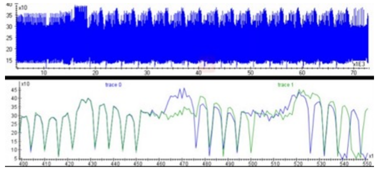
Passive attacks



Key Leakages

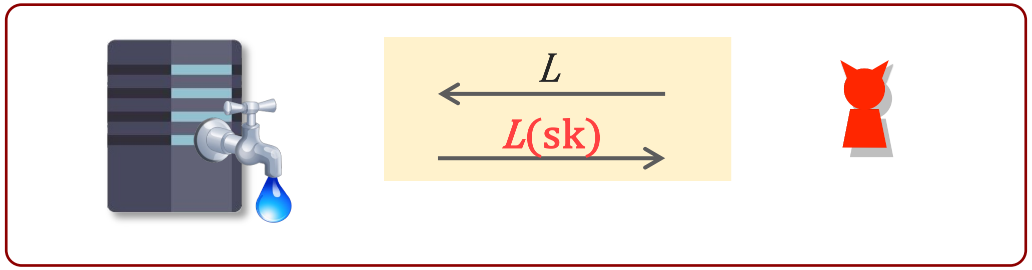
Leakage & Tampering Attacks

Key Leakage



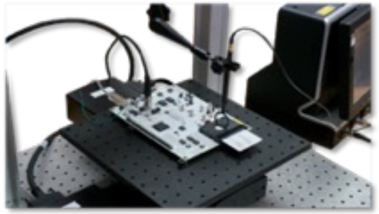
Side-Channel Attacks
- Power
- Time
- Sound
- …

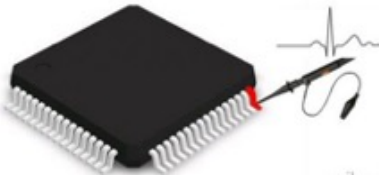
Passive attacks



Key Leakages

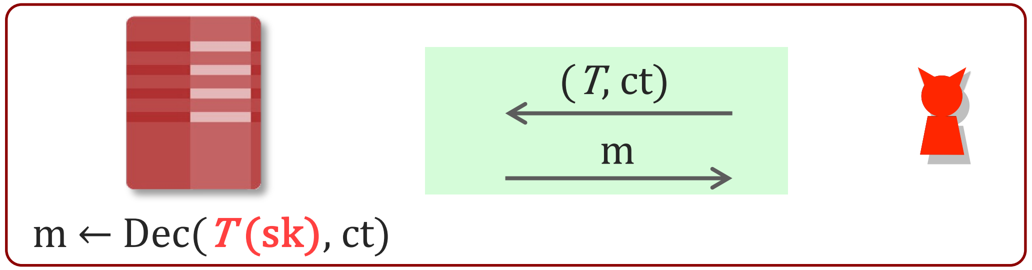
Key Tampering





- Fault injection
- Memory tampering
- …

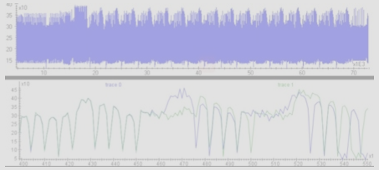
Active attacks

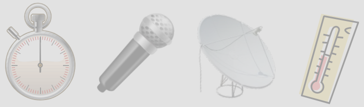


Operating under **Tampered keys**

Leakage & Tampering Attacks

Key Leakage

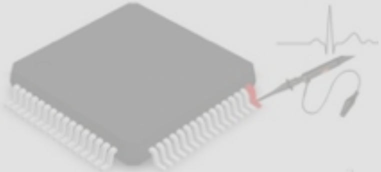




Side-Channel Attacks
- Power
- Time
- Sound
- …

Passive attacks

Key Tampering



- Fault injection
- Memory tampering
- …

Active attacks

How to achieve security resilient to both Leakage & Tampering attacks?

Security Resilient to Both Leakage & Tampering Attacks

① CTL model (Continual Tampering & Leakage) [Kalai et al., C11]

+ **Strong** security guarantee: Continual tampering & leakage attacks
- Require **additional mechanisms**: Key-updating or Self-destruct

Schemes	Efficiency
SIG [Kalai et al., C11]	|signature| > **20** group elements
CCA-PKE [Fujisaki-Xagawa, AC16]	|ciphertext| > **8** group elements

- Rely on **heavy tools**:

tSE-NIZK (true-Simulation Extractable NIZK) [Dodis et al., AC10]

or OT-LF (One-Time Lossy Filter) [Qin-Liu, AC13]

Security Resilient to Both Leakage & Tampering Attacks

② BLT model (Bounded Leakage & Tampering) [Damgård et al., AC13]

- **Mild** security guarantee:
  - **Leakage**: Bounded amount [Naor-Segev, C09]
  - **Tampering**: Bounded number, No post-challenge, Arbitrary functions

\+ **No additional mechanisms**

Schemes	Efficiency
SIG [Faonio-Venturi, AC16] [Dodis et al., AC10]	|signature| > **34** group elements
CCA-PKE [Faonio-Venturi, AC16] [Qin-Liu, AC13]	|ciphertext| > **19** group elements

\- Rely on **heavy tools**: tSE-NIZK or OT-LF

Security Resilient to Both Leakage & Tampering Attacks

③ sLTR model (strong Leakage & Tampering-Resilience) [Sun et al., ACNS19]

- **Mild** security guarantee:
  - **Leakage**: Bounded amount [Naor-Segev, C09]
  - **Tampering**: Unbounded number, Allow post-challenge tampering, For specific functions (e.g., $\mathcal{T}_{\text{affine}}$) [Bellare-Kohno, EC03]

\+ **No additional mechanisms**

Schemes	Efficiency
CCA-PKE [Sun et al., ACNS19]	|ciphertext| > **20** group elements

\- Rely on **heavy tools**: tSE-NIZK

Security Resilient to Both Leakage & Tampering Attacks

④ pcBLT model (post-challenge BLT)

[Chakraborty-Rangan, CT-RSA19]

- **Mild** security guarantee:
  - **Leakage**: Bounded amount
  - **Tampering**: Bounded number, Allow post-challenge tampering,
    For arbitrary functions

- Require **additional mechanisms**: Split-state

Schemes	Efficiency
CCA-PKE [Chakraborty-Rangan, CT-RSA19]	|ciphertext| > **20** group elements

- Rely on **heavy tools**: tSE-NIZK

Security Resilient to Both Leakage & Tampering Attacks

Schemes	Efficiency	Model
SIG [Kalai et al., C11]	|signature| > **20** group elements	CTL
CCA-PKE [Fujisaki-Xagawa, AC16]	|ciphertext| > **8** group elements	CTL
SIG [Faonio-Venturi, AC16] [Dodis et al., AC10]	|signature| > **34** group elements	BLT
CCA-PKE [Faonio-Venturi, AC16] [Qin-Liu, AC13]	|ciphertext| > **19** group elements	BLT
CCA-PKE [Sun et al., ACNS19]	|ciphertext| > **20** group elements	sLTR
CCA-PKE [Chakraborty-Rangan, CT-RSA19]	|ciphertext| > **20** group elements	pcBLT

All rely on somewhat **heavy tools** like tSE-NIZK or OT-LF!

Security Resilient to Both Leakage & Tampering Attacks

Schemes	Efficiency	Model
SIG [Kalai et al., C11]	|signature| > **20** group elements	CTL
CCA-PKE [Fujisaki-Xagawa, AC16]	|ciphertext| > **8** group elements	CTL
SIG [Faonio-Venturi, AC16] [Dodis et al., AC10]	|signature| > **34** group elements	BLT
CCA-PKE [Faonio-Venturi, AC16] [Qin-Liu, AC13]	|ciphertext| > **19** group elements	BLT
CCA-PKE [Sun et al., ACNS19]	|ciphertext| > **20** group elements	sLTR
CCA-PKE [Chakraborty-Rangan, CT-RSA19]	|ciphertext| > **20** group elements	pcBLT

All rely on somewhat **heavy tools** like tSE-NIZK or OT-LF!

How to achieve security resilient to both Leakage & Tampering attacks, More efficiently?

Contributions: More Efficient SIG and CCA-PKE in the LTR Setting

Schemes	Efficiency	Model
SIG [Kalai et al., C11]	|signature| > **20** group elements	CTL
CCA-PKE [Fujisaki-Xagawa, AC16]	|ciphertext| > **8** group elements	CTL
SIG [Faonio-Venturi, AC16] [Dodis et al., AC10]	|signature| > **34** group elements	BLT
CCA-PKE [Faonio-Venturi, AC16] [Qin-Liu, AC13]	|ciphertext| > **19** group elements	BLT
CCA-PKE [Sun et al., ACNS19]	|ciphertext| > **20** group elements	sLTR
CCA-PKE [Chakraborty-Rangan, CT-RSA19]	|ciphertext| > **20** group elements	pcBLT
Our SIG	|signature| = **4** group elements	sLTR
Our CCA-PKE	|ciphertext| = **6** group elements	sLTR

5~8× shorter

1.3~3.3× shorter

Contributions: More Efficient SIG and CCA-PKE in the LTR Setting

Schemes	Efficiency	Model
Our SIG	|signature| = 4 group elements (5~8× shorter)	sLTR
Our CCA-PKE	|ciphertext| = 6 group elements (1.3~3.3× shorter)	sLTR

Features

- **Direct** construction over asymmetric pairing groups
- Based on the standard MDDH (including SXDH, k-Linear) assumptions
- In the standard model
- **Leakage** rate: **1/4 – o(1)** (our SIG) or **1/3 – o(1)** (our CCA-PKE)
- **Tampering** functions: **affine functions** $\mathcal{T}_{\text{affine}}$

Contents

Recap: sLTR model for PKE [Sun et al., ACNS19]

Challenger $\mathcal{C}$ | Adversary $\mathcal{A}$

pp ← Setup
(pk, sk) ← Gen(pp) — (pp, pk) →

Leakage queries
← L
L(sk) →

Decryption queries under **Tampered keys**
m ← Dec(T(sk), ct) — ← (T, ct)
m →

β ← {0,1} — ← (m_0, m_1)
ct* ← Enc(pk, m_β) — ct* →

Post-Challenge Decryption queries under **Tampered keys**
m ← Dec(T(sk), ct) — ← (T, ct)
If (T, ct) = (id. fun., ct*)
m := ⊥ — m →

← β'

Minimal restriction!

sLTR–CCA security:

| Pr[β'= β] — 1/2 |

= negligible

sLTR model (strong Leakage & Tampering-Resilience) for SIG

Challenger $\mathcal{C}$ | Adversary $\mathcal{A}$

$\text{pp} \leftarrow \text{Setup}$

$(\text{vk}, \text{sk}) \leftarrow \text{Gen}(\text{pp})$ → (pp, vk) →

Leakage queries

← L

$L(\text{sk})$ →

Signing queries under **Tampered keys**

← (T, m)

$\sigma \leftarrow \text{Sign}(T(\text{sk}), \text{m})$

If $T =$ identity func. $Q_{\text{id}} := Q_{\text{id}} \cup \{(\text{m}, \sigma)\}$

σ →

Signing under **original** keys

← (m^*, σ^*)

$\mathcal{A}$ **wins**: $\text{Vrfy}(\text{vk}, \text{m}^*, \sigma^*) = 1 \ \wedge \ (\text{m}^*, \sigma^*) \notin Q_{\text{id}}$

sLTR–CMA security: $\Pr[\mathcal{A}$ **wins**$]$ = negligible

Minimal restriction!

Strong existential unforgeability!

- **Counterpart to the sLTR model for PKE** [Sun et al., ACNS19]
  - **Leakage**: Bounded amount [Naor-Segev, C09]
  - **Tampering**: Unbounded number, For specific functions [Bellare-Kohno, EC03]
  - \+ **No additional mechanisms**

Contents

More Efficient & Direct Construction of SIG

Setup $\to$ pp $= ([\mathbf{U}], [\mathbf{K}_0\mathbf{U}], [\mathbf{K}_1\mathbf{U}], [\mathbf{A}], [\mathbf{A}^\top\mathbf{K}_0], [\mathbf{A}^\top\mathbf{K}_1])$, with $\mathbf{U}, \mathbf{A} \in \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Gen $\to$ (vk, sk): $\mathrm{sk} = \mathbf{K}$, $\mathrm{vk} = [\mathbf{A}^\top\mathbf{K}]$, with $\mathbf{K} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Sign(sk $= \mathbf{K}$, m) $\to \sigma$:

$[\mathbf{c}] := [\mathbf{U}]\,\mathbf{w}$ with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

sk $= \mathbf{K}$

$[\mathbf{K}_0\mathbf{U}], [\mathbf{K}_1\mathbf{U}]$ in pp

$\tau := \mathrm{H}(\mathrm{vk}, \mathrm{m}, [\mathbf{c}])$

$[\mathbf{d}] := \mathbf{K}\,[\mathbf{c}] + [(\mathbf{K}_0+\tau\cdot\mathbf{K}_1)\,\mathbf{U}]\,\mathbf{w}$

output $\sigma = ([\mathbf{c}], [\mathbf{d}])$

Vrfy(vk $= [\mathbf{A}^\top\mathbf{K}]$, m, $\sigma = ([\mathbf{c}], [\mathbf{d}])$) $\to 1/0$:

$[\mathbf{c}] \neq [\mathbf{0}]$

vk $= [\mathbf{A}^\top\mathbf{K}]$

$[\mathbf{A}^\top\mathbf{K}_0], [\mathbf{A}^\top\mathbf{K}_1]$ in pp

$\tau := \mathrm{H}(\mathrm{vk}, \mathrm{m}, [\mathbf{c}])$

output 1 iff

$e([\mathbf{A}^\top], [\mathbf{d}]) = e([\mathbf{A}^\top\mathbf{K}], [\mathbf{c}]) + e([\mathbf{A}^\top(\mathbf{K}_0+\tau\cdot\mathbf{K}_1)], [\mathbf{c}])$

More Efficient & Direct Construction of SIG

Setup → pp = ([**U**], [**K**$_0$**U**], [**K**$_1$**U**], [**A**], [**A**$^\top$**K**$_0$], [**A**$^\top$**K**$_1$]), with **U**, **A** $\in \mathbb{Z}_p^{(k+1)\times k}$, **K**$_0$, **K**$_1$ $\in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Gen → (vk, sk): sk = **K**, vk = [**A**$^\top$**K**], with **K** $\in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Leakage & Tampering on K, but not on K$_0$, K$_1$

Sign(sk = **K**, m) → σ:

[**c**] := [**U**] **w** with **w** ← $\mathbb{Z}_p^k$

sk = **K**

[**K**$_0$**U**], [**K**$_1$**U**] in pp

τ := H(vk, m, [**c**])

[**d**] := **K** [**c**] **+** [(**K**$_0$+τ·**K**$_1$) **U**] **w**

output σ = ([**c**], [**d**])

Carefully Integrate the two components

Vrfy(vk = [**A**$^\top$**K**], m, σ = ([**c**], [**d**])) → 1/0:

[**c**] ≠ [**0**]

vk = [**A**$^\top$**K**]

[**A**$^\top$**K**$_0$], [**A**$^\top$**K**$_1$] in pp

τ := H(vk, m, [**c**])

output 1 iff

e([**A**$^\top$], [**d**])

= e([**A**$^\top$**K**], [**c**]) **+** e([**A**$^\top$(**K**$_0$+τ·**K**$_1$)], [**c**])

Construction of SIG: The First Component

First Component (related to K)

Gen → (vk, sk): $sk = \mathbf{K}$, $vk = [\mathbf{A}^\top \mathbf{K}]$, with $\mathbf{K} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Sign($sk = \mathbf{K}$, m) → σ:

$[\mathbf{c}] := [\mathbf{U}]\,\mathbf{w}$ with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

$sk = \mathbf{K}$

$[\mathbf{d}] := \mathbf{K}\,[\mathbf{c}]$

output $\sigma = ([\mathbf{c}], [\mathbf{d}])$

Vrfy($vk = [\mathbf{A}^\top \mathbf{K}]$, m, $\sigma = ([\mathbf{c}], [\mathbf{d}])$) → 1/0:

$[\mathbf{c}] \neq [\mathbf{0}]$

$vk = [\mathbf{A}^\top \mathbf{K}]$

output 1 iff

$e([\mathbf{A}^\top], [\mathbf{d}])$

$= e([\mathbf{A}^\top \mathbf{K}], [\mathbf{c}])$

Construction of SIG: The First Component

First Component (related to K)

Gen → (vk, sk): $\mathrm{sk} = \mathbf{K}$, $\mathrm{vk} = [\mathbf{A}^\top \mathbf{K}]$, with $\mathbf{K} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Sign($\mathrm{sk} = \mathbf{K}$, m) → σ:

$[\mathbf{c}] := [\mathbf{U}]\,\mathbf{w}$ with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

$\mathrm{sk} = \mathbf{K}$ →

$[\mathbf{d}] := \mathbf{K}\,[\mathbf{c}]$

output $\sigma = ([\mathbf{c}], [\mathbf{d}])$

Vrfy($\mathrm{vk} = [\mathbf{A}^\top \mathbf{K}]$, m, $\sigma = ([\mathbf{c}], [\mathbf{d}])$) → 1/0:

$[\mathbf{c}] \neq [\mathbf{0}]$

$\mathrm{vk} = [\mathbf{A}^\top \mathbf{K}]$ →

output 1 iff

$e([\mathbf{A}^\top], [\mathbf{d}]) = e([\mathbf{A}^\top \mathbf{K}], [\mathbf{c}])$

⟺ **Equivalent to $[\mathbf{d}] = \mathbf{K}\,[\mathbf{c}]$ under MDDH**

Construction of SIG: The First Component

First Component (related to K)

Gen → (vk, sk): sk = $\mathbf{K}$, vk = $[\mathbf{A}^\top \mathbf{K}]$, with $\mathbf{K} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

Sign(sk = $\mathbf{K}$, m) → σ:

$[\mathbf{c}] := [\mathbf{U}]\,\mathbf{w}$ with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

sk = $\mathbf{K}$ →

$[\mathbf{d}] := \mathbf{K}\,[\mathbf{c}]$

output σ = ([**c**], [**d**])

Vrfy(vk = $[\mathbf{A}^\top \mathbf{K}]$, m, σ = ([**c**], [**d**])) → 1/0:

$[\mathbf{c}] \neq [\mathbf{0}]$

vk = $[\mathbf{A}^\top \mathbf{K}]$ →

output 1 iff

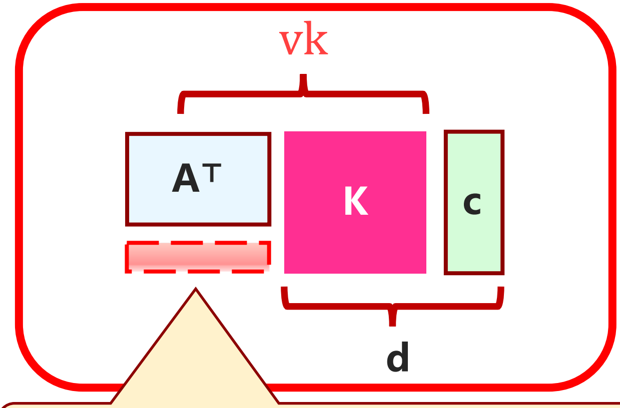
$e([\mathbf{A}^\top], [\mathbf{d}]) = e([\mathbf{A}^\top \mathbf{K}], [\mathbf{c}])$

Equivalent to $[\mathbf{d}] = \mathbf{K}\,[\mathbf{c}]$ under MDDH

Security against No-Message Attacks (No Signing Queries) under Key Leakages

- Given **only** vk = $[\mathbf{A}^\top \mathbf{K}]$, it is hard to produce σ = ([**c**], [**d**]) to pass Vrfy:

$$[\mathbf{c}] \neq [\mathbf{0}] \quad \wedge \quad [\mathbf{d}] = \mathbf{K}\,[\mathbf{c}]$$



Leftover Entropy of sk = $\mathbf{K}$

- … even in the presence of additional **leakage** $L(\text{sk}) = L(\mathbf{K})$

Construction of SIG: The Second Component

First Component (related to K) | **Second Component (related to K_0, K_1)**

Setup → pp = $([\mathbf{U}], [\mathbf{K}_0\mathbf{U}], [\mathbf{K}_1\mathbf{U}], [\mathbf{A}], [\mathbf{A}^\top\mathbf{K}_0], [\mathbf{A}^\top\mathbf{K}_1])$, with $\mathbf{U}, \mathbf{A} \in \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(k+1)\times(k+1)}$

$\mathrm{Sign}(sk = \mathbf{K}, m) \to \sigma$:

$[\mathbf{c}] := [\mathbf{U}]\,\mathbf{w}$ with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

$sk = \mathbf{K}$

$[\mathbf{K}_0\mathbf{U}], [\mathbf{K}_1\mathbf{U}]$ in pp

$\tau := H(vk, m, [\mathbf{c}])$

$[\mathbf{d}] := \mathbf{K}\,[\mathbf{c}] + [(\mathbf{K}_0+\tau\cdot\mathbf{K}_1)\,\mathbf{U}]\,\mathbf{w}$

output $\sigma = ([\mathbf{c}], [\mathbf{d}])$

$\mathrm{Vrfy}(vk = [\mathbf{A}^\top\mathbf{K}], m, \sigma = ([\mathbf{c}], [\mathbf{d}])) \to 1/0$:

$[\mathbf{c}] \neq [\mathbf{0}]$

$vk = [\mathbf{A}^\top\mathbf{K}]$

$[\mathbf{A}^\top\mathbf{K}_0], [\mathbf{A}^\top\mathbf{K}_1]$ in pp

$\tau := H(vk, m, [\mathbf{c}])$

output 1 iff

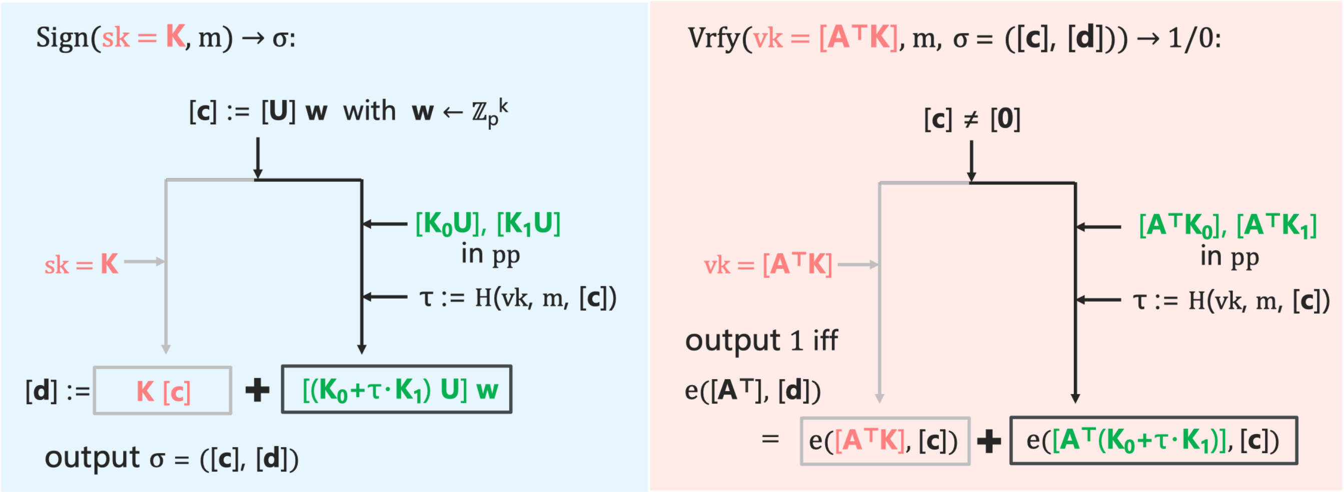
$e([\mathbf{A}^\top], [\mathbf{d}])$

$= e([\mathbf{A}^\top\mathbf{K}], [\mathbf{c}]) + e([\mathbf{A}^\top(\mathbf{K}_0+\tau\cdot\mathbf{K}_1)], [\mathbf{c}])$

Construction of SIG: The Second Component

Second Component (related to K_0, K_1)

Setup → pp = ([**U**], [K_0**U**], [K_1**U**], [**A**], [$\mathbf{A}^\top K_0$], [$\mathbf{A}^\top K_1$]), with **U**, **A** $\in \mathbb{Z}_p^{(k+1)\times k}$, $K_0, K_1 \in \mathbb{Z}_p^{(k+1)\times(k+1)}$



Masking First Component during Signing Queries under Tampered Keys

- Essentially the **OTSS-NIZK** (One-Time Simulation-Sound NIZK) proposed in [Kiltz-Wee, EC15]
- … but **OTSS** is **insufficient**: multiple signing queries contain multiple NIZK proofs
- We resort to another property as observed in [Kiltz-Wee, EC15]:

  randomized PRF on τ

  which can mask First Component

Security of SIG: Putting Two Components Together

First Component (related to K) + Second Component (related to K_0, K_1)

Security against No-Message Attacks (No Signing Queries) under Key Leakages

Masking First Component during Signing Queries under Tampered Keys

sLTR-CMA security for SIG

under Key Leakages & Tampered Keys

Contents

More Efficient & Direct Construction of CCA-PKE

Setup → pp = ([**U**], [$\mathbf{K}_0\mathbf{U}$], [$\mathbf{K}_1\mathbf{U}$], [**A**], [$\mathbf{A}^\top\mathbf{K}_0$], [$\mathbf{A}^\top\mathbf{K}_1$]), with **U**, **A** $\in \mathbb{Z}_p^{(k+2)\times k}$, $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_p^{(k+1)\times(k+2)}$

Gen → (pk, sk): sk = **k**, pk = [$\mathbf{k}^\top\mathbf{U}$], with $\mathbf{k} \in \mathbb{Z}_p^{k+2}$

Enc(pk = [$\mathbf{k}^\top\mathbf{U}$], m) → ct:

[**c**] := [**U**] **w** with $\mathbf{w} \leftarrow \mathbb{Z}_p^k$

pk = [$\mathbf{k}^\top\mathbf{U}$]

[$\mathbf{K}_0\mathbf{U}$], [$\mathbf{K}_1\mathbf{U}$] in pp

τ := H(pk, [**c**], [**d**])

[**d**] := [$\mathbf{k}^\top\mathbf{U}$] **w** + m [**e**] := [($\mathbf{K}_0$+τ·$\mathbf{K}_1$) **U**] **w**

output ct = ([**c**], [**d**], [**e**])

Dec(sk = **k**, ct = ([**c**], [**d**], [**e**])) → m/⊥:

[**c**]

sk = **k**

[$\mathbf{A}^\top\mathbf{K}_0$], [$\mathbf{A}^\top\mathbf{K}_1$] in pp

τ := H(pk, [**c**], [**d**])

output

m := [**d**] - $\mathbf{k}^\top$[**c**]

iff e([$\mathbf{A}^\top$], [**e**]) = e([$\mathbf{A}^\top$($\mathbf{K}_0$+τ·$\mathbf{K}_1$)], [**c**])

More Efficient & Direct Construction of CCA-PKE

Setup → pp = ([**U**], [**K**$_0$**U**], [**K**$_1$**U**], [**A**], [**A**$^\top$**K**$_0$], [**A**$^\top$**K**$_1$]), with **U**, **A** $\in \mathbb{Z}_p^{(k+2)\times k}$, **K**$_0$, **K**$_1$ $\in \mathbb{Z}_p^{(k+1)\times(k+2)}$

Gen → (pk, sk): sk = **k**, pk = [**k**$^\top$**U**], with **k** $\in \mathbb{Z}_p^{k+2}$

Leakage & Tampering on **k**, but not on **K**$_0$, **K**$_1$

Enc(pk = [**k**$^\top$**U**], m) → ct:

[**c**] := [**U**] **w** with **w** ← $\mathbb{Z}_p^k$

pk = [**k**$^\top$**U**] →

[**K**$_0$**U**], [**K**$_1$**U**] in pp

τ := H(pk, [**c**], [**d**])

Hide the message

[**d**] := [**k**$^\top$**U**] **w** + m   [**e**] := [(**K**$_0$+τ·**K**$_1$) **U**] **w**

Prove the well-formedness

output ct = ([**c**], [**d**], [**e**])

Dec(sk = **k**, ct = ([**c**], [**d**], [**e**])) → m/⊥:

[**c**]

sk = **k** →

[**A**$^\top$**K**$_0$], [**A**$^\top$**K**$_1$] in pp

τ := H(pk, [**c**], [**d**])

output

m := [**d**] - **k**$^\top$[**c**]

iff e([**A**$^\top$], [**e**]) = e([**A**$^\top$(**K**$_0$+τ·**K**$_1$)], [**c**])

Security of PKE: Putting Two Components Together

First Component (related to k) + **Second Component (related to K_0, K_1)**

CPA Security under Key Leakages

Reject Decryption Queries under Tampered Keys

sLTR-CCA security for PKE under Key Leakages & Tampered Keys

Conclusion

- **More Efficient** SIG and CCA-PKE with leakage & tamper resilience
  - ✓ Direct construction, avoid using tSE-NIZK

Schemes	Efficiency	Model
Our SIG	|signature| = **4** group elements (*5~8× shorter*)	sLTR
Our CCA-PKE	|ciphertext| = **6** group elements (*1.3~3.3× shorter*)	sLTR

- New **sLTR security for SIG**: counterpart to the sLTR security for PKE
- The first SIG with **strong existential unforgeability** in the LTR setting

Thanks! Questions?

ePrint: ia.cr/2023/1965