KU LEUVEN

TIRAMISU: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model

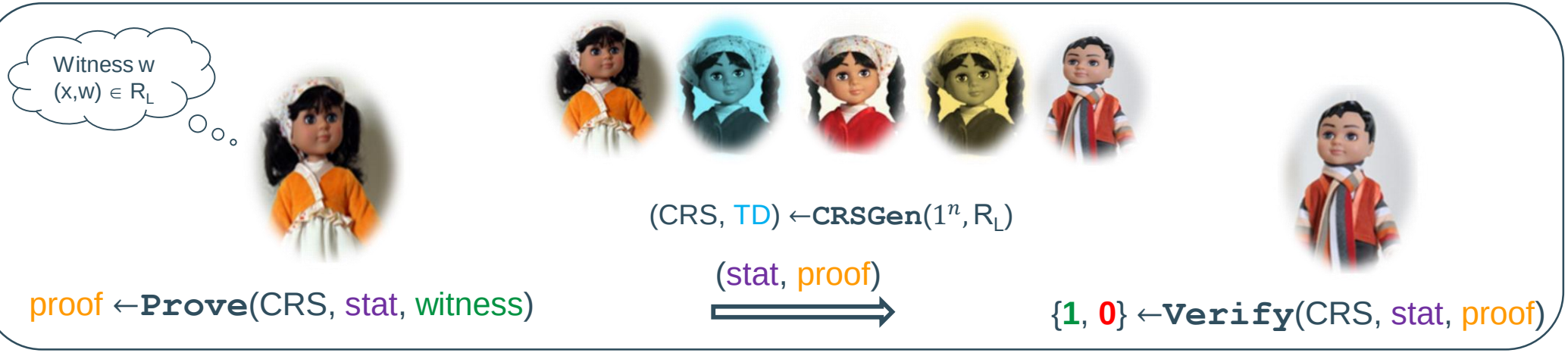
Karim Baghery [1,2] and Mahdi Sedaghat [1]

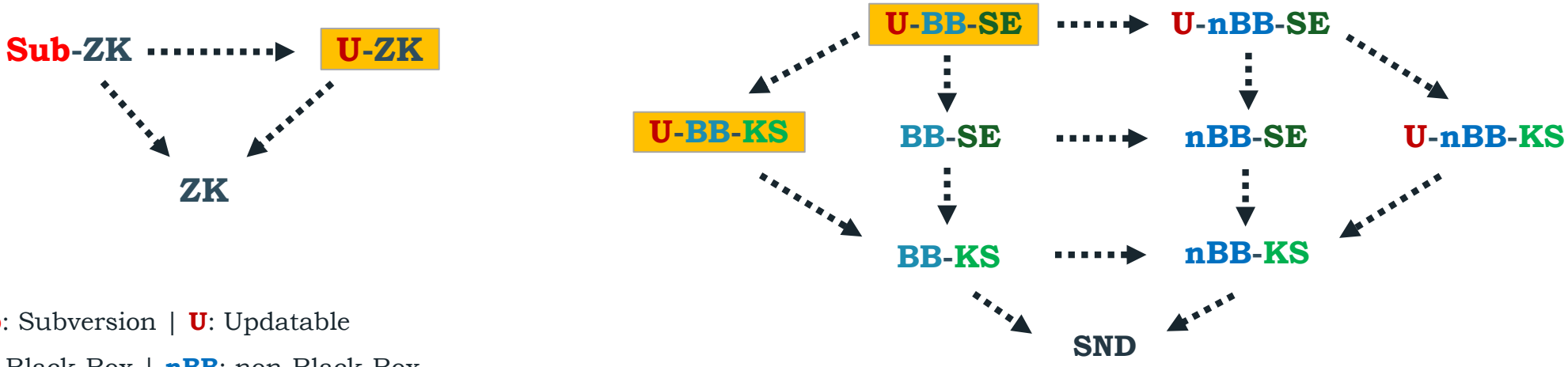
[1]imec-COSIC, KU Leuven, Leuven, Belgium
[2]University of Tartu, Tartu, Estonia.

karim.baghery@kuleuven.be
ssedagha@esat.kuleuven.be

ia.cr/2020/474

Overview on Tiramisu & (Sub./Upd.) NIZKs in the CRS Model:





Sub: Subversion | **U**: Updatable

BB: Black-Box | **nBB**: non-Black-Box

ZK: Zero-knowledge | **SND**: Soundness | **KS**: Knowledge Sound | **SE**: Simulation Extractable

[PHGR13]

[BCG+15, ABL+19]

COCO [KZM+15]

[Gro16]

[BFS16]
[ABLZ17]
[Fuc18]

[GM17, AB19]

[GKM+18]

[Bag19a]

[Bag19b]

Lamassu [ARS20]

Tiramisu [BS20]

Tiramisu: Building U-ZK and U-BB-SE NIZKs (zk-SNARKs)

Sub/U-ZK and U-nBB-SE SNARK (e.g. [ARS20])

Tiramisu [BS20]
[Bag19a], [Bag19b], [ARS20]

U-ZK and U-BB-SE NIZK (SNARK)

- Given a language $\boldsymbol{L}$ with the NP relation $\mathbf{R}_{\boldsymbol{L}}$, define $\boldsymbol{L}'$ s. t. $\big((x, c, pk_i), (w, r)\big) \in \boldsymbol{R}_{\boldsymbol{L}'}$ iff:

$$c = Enc(pk_i, w; r)) \bigwedge \big((x, w) \in \boldsymbol{R}_{\boldsymbol{L}}\big)$$

  - $\Pi_{\text{enc}} \coloneqq (\text{KG}, \text{Enc}, \text{Dec})$ is CPA secure public-key cryptosystem with *updatable keys* $(\text{pk}_\text{i}, \text{sk}_\text{i})$

- Updatable public-key cryptosystems: can be constructed from key-homomorphic encryption schemes [AHI11] (a variation of El-Gamal [ElG84] instantiated in the pairing-based groups)
  - Similar to updatable NIZK arguments [GKM+18]
  - and updatable signatures [ARS20]

Tiramisu in Comparison with Current Constructions:

- Upd. **BB** Sim. Ext. & **Upd**-ZK NIZKs (SNARKs) [Tiramisu, BS20]
- **Upd.** nBB Sim. Ext. & Sub-ZK SNARK [Lamassu, ARS20]
- nBB Sim. Ext. & **Sub**-ZK SNARK [Bag19b, Lip19]
- **BB** Sim. Ext. NIZKs (zk-SNARK) [KZM+15, Bag19a]
- nBB **Sim. Ext.** zk-SNARK [GM17, BG18, AB19]
- **nBB** Knowledge Sound zk-SNARKs [e.g. Gro16]

In Italian, Tiramisù literally means "lift me up", or more literally "pull it up".

	Zero-Knowledge			Simulation Extractability			
	ZK	U-ZK	Sub-ZK	nBB-SE	BB-SE	U-nBB-SE	U-BB-SE
Tiramisu	✓	✓	×	✓	✓	✓	✓
CØCØ [KZM+15, Bag19a]	✓	×	×	✓	✓	×	×
[GM17, BG18, AB19]	✓	×	×	✓	×	×	×
[Bag19b, Lip19]	✓	✓	✓	✓	×	×	×
[ARS20a]	✓	✓	✓*	✓	×	✓	×

KU LEUVEN

Thank You!

karim.baghery@kuleuven.be
ssedagha@esat.kuleuven.be

CØCØ Framework: Building BB-SE NIZKs (zk-SNARKs)

(nBB Knowledge) Sound NIZK (zk-SNARK)

CØCØ Framework [KZM+15]

Black-Box Sim. Ext. NIZK (zk-SNARK)

- Given a language $\boldsymbol{L}$ with the corresponding NP relation $\mathbf{R}_{\boldsymbol{L}}$, defines a new language $\boldsymbol{L}'$ such that $\left((x, c, \mu, pk_s, pk_e, \rho), (w, r, r_0, s_0)\right) \in \boldsymbol{R}_{\boldsymbol{L}'}$ iff:

$$\underbrace{c = Enc(pk_e, w; r)}_{\text{Black-Box Extraction}} \bigwedge \left((x, w) \in \boldsymbol{R}_{\boldsymbol{L}} \bigvee \left(\underbrace{\mu = f_{s_0}(pk_s) \bigwedge \rho = Com(s_0, r_0)}_{\text{Simulation Sound or nBB Simulation Extractable}} \right) \right)$$

  - $Enc(.)$ is a semantically secure encryption scheme,
  - $f_{s_0}(.): \{0,1\}^* \rightarrow \{0,1\}^{\lambda}$ is a PRF family,
  - $Com(.)$ is a perfectly binding commitment scheme.

- Used in several UC-secure protocols [Gro06]: Hawk [KMS+16], Gyges [JKS16], Ouroboros Crypsinous [KKKZ19], …

[Bag19b, ARS20]: Building Sub-ZK & nBB-SE/U-nBB-SE zk-SNARKs

Sub-ZK and nBB Knowledge Sound SNARK e.g. [ABLZ17, Fuc18]

[Bag19b]
[BG90, KZM+15]

Sub-ZK & nBB-SE SNARK

- Given a language $\boldsymbol{L}$ with the corresponding NP relation $\mathbf{R}_{\boldsymbol{L}}$, define a new language $\boldsymbol{L}'$ such that $\left((x, \cancel{c,} \mu, pk_s, \cancel{pk_e,} \rho), (w, \cancel{r,} r_0, s_0)\right) \in \boldsymbol{R}_{\boldsymbol{L}'}$ iff:

$$\cancel{c = Enc(pk_e, w; r)} \bigwedge \left((x,w) \in \boldsymbol{R}_{\boldsymbol{L}} \bigvee \left(\mu = f_{s_0}(pk_s) \bigwedge \rho = Com(s_0, r_0) \right) \right)$$

Sub-ZK and Updatable nBB Knowledge Sound SNARK e.g. [GKM+18]

[ARS20, Lamassu]
[DS16, Bag19b]

Sub-ZK & U-nBB-SE SNARK

- Given a language $\boldsymbol{L}$ with the corresponding NP relation $\mathbf{R}_{\boldsymbol{L}}$, defines a new language $\boldsymbol{L}'$ such that $\left((x, cpk, pk), (w, csk - sk)\right) \in \boldsymbol{R}_{\boldsymbol{L}'}$ iff:

$$(x,w) \in \boldsymbol{R}_{\boldsymbol{L}} \bigvee (\mathrm{cpk} = \mathrm{pk} \cdot \mu(\mathrm{csk} - sk))$$

  - $(\mathrm{cpk}, \mathrm{csk})$ of a key-homomorphic signature
  - $(\mathrm{pk}, \mathrm{sk})$ of a one-time secure signature
  - μ: $\mathrm{SK} \rightarrow PK$ (e.g. $\mathrm{pk} = g^{\mathrm{sk}}$).