Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model
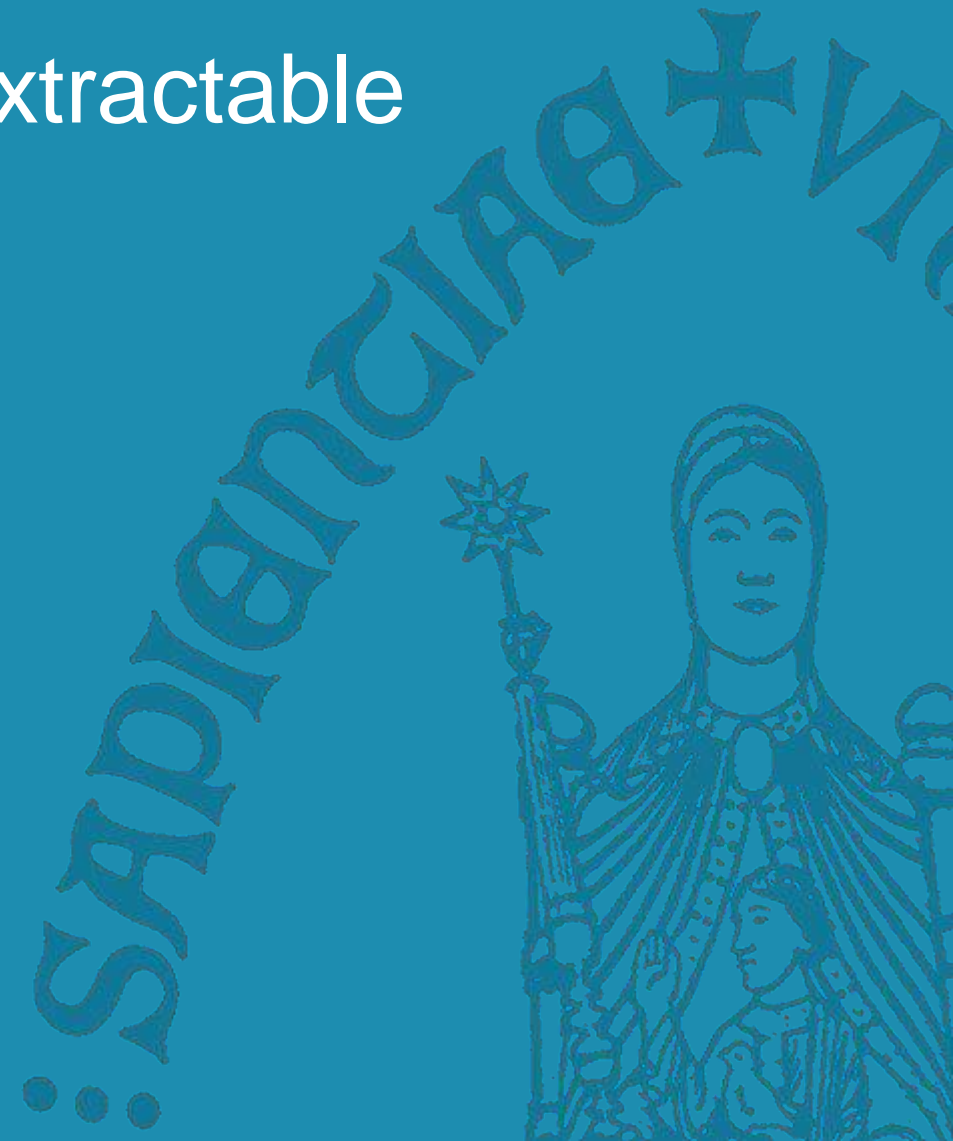
Karim Baghery [1,2] and Mahdi Sedaghat [1]
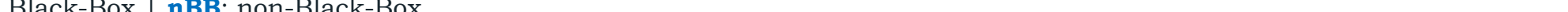
[1]imec-COSIC, KU Leuven, Leuven, Belgium
[2]University of Tartu, Tartu, Estonia.

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

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

Witness w
$(x, w) \in R_L$

proof $\leftarrow$ **Prove**(CRS, stat, witness)

$(CRS, TD) \leftarrow$ **CRSGen**$(1^n, R_L)$

(stat, proof)

$\{1, 0\} \leftarrow$ **Verify**(CRS, stat, proof)

Sub-ZK $\cdots\cdots\rightarrow$ U-ZK

ZK

U-BB-SE $\cdots\cdots\rightarrow$ U-nBB-SE

U-BB-KS   BB-SE $\cdots\cdots\rightarrow$ nBB-SE   U-nBB-KS

BB-KS $\cdots\cdots\rightarrow$ nBB-KS

SND

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]

KU LEUVEN

C∅C∅ Framework: Building BB-SE NIZKs (zk-SNARKs)

$$\boxed{\text{(nBB Knowledge) Sound NIZK (zk-SNARK)}} \rightarrow \boxed{\text{C∅C∅ Framework [KZM+15]}} \rightarrow \boxed{\text{Black-Box Sim. Ext. NIZK (zk-SNARK)}}$$

➢ Given a language L with the corresponding NP relation R_L, defines a new language L' such that $\big((x, c, \mu, pk_s, pk_e, \rho), (w, r, r_0, s_0)\big) \in R_{L'}$ iff:

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

Black-Box Extraction

Simulation Sound or nBB Simulation Extractable

- $Enc(.)$ 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], …

KU LEUVEN

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

$$\cancel{c = Enc(pk_e, w; r))} \bigwedge \left((x, w) \in \mathbf{R}_L \bigvee \left(\mu = f_{s_0}(pk_s) \bigwedge \rho = Com(s_0, r_0)\right)\right)$$
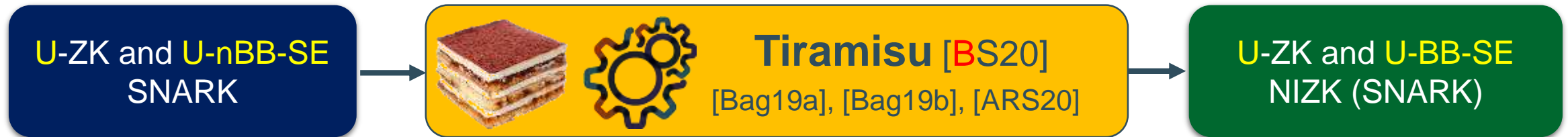
Sub-ZK and Updatable nBB Knowledge Sound SNARK e.g. [GKM+18]	→	**[ARS20, Lamassu]** [DS16, Bag19b]	→	Sub-ZK & U-nBB-SE SNARK

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

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

$$(x, w) \in \mathbf{R}_L \bigvee (cpk = pk \cdot \mu(csk - sk))$$

KU LEUVEN

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

| U-ZK and U-nBB-SE SNARK | → | Tiramisu [BS20] [Bag19a], [Bag19b], [ARS20] | → | U-ZK and U-BB-SE NIZK (SNARK) |

➢ Given a language L with the NP relation R_L, define L' s. t. $\big((x, c, pk_i), (w, r)\big) \in R_{L'}$ iff:

$$c = Enc(pk_i, w; r)) \bigwedge ((x, w) \in R_L)$$

▪ $\Pi_{enc} := (KG, Enc, Dec)$ is CPA secure public-key cryptosystem with *updatable keys* (pk_i, sk_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]

KU LEUVEN

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	✓	✓	✗	✓	✓	✓	✓
C0C0 [KZM+15] [Bag19a]	✓	✗	✗	✓	✓	✗	✗
[GM17] [BG18] [AB19]	✓	✗	✗	✓	✗	✗	✗
[Bag19b] [Lip19]	✓	✓	✓	✓	✗	✗	✗
[ARS20a]	✓	✓	✓*	✓	✗	✓	✗

KU LEUVEN

Thank You!

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