Non-Interactive and Reusable UC Commitments with Adaptive Security

Marc Fischlin[1], Benoit Libert[2], *Mark Manulis*[1]

[1]TU Darmstadt & CASED, Germany

[2]University catholique de Louvain, Belgium

CRYPTO
CRYPTOGRAPHIC PROTOCOLS

Commitment Schemes

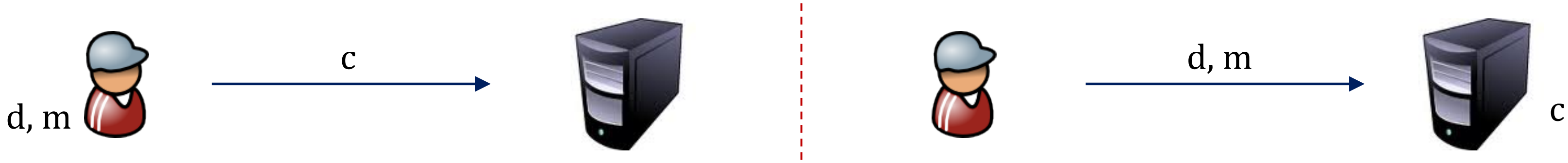
Commitments belong to fundamental building blocks in cryptography:

imply key exchange, oblivious transfer [DG03]
secure two and multi-party computation [CLOS02]

used in digital auctions, voting, e-cash systems

two phases

commit **open**



hiding : c leaks no info about m

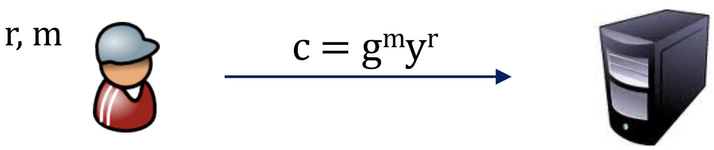
c cannot be opened to m‘ : binding

security goals

Example: Pedersen Commitments [Ped01]

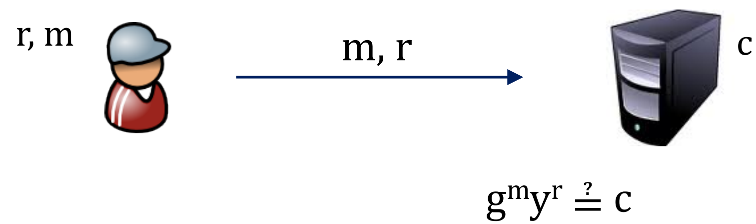
DL-hard group $\mathbb{G} = \langle g \rangle$ of prime order q public key $y = g^x$ for some $x \in_R \mathbb{Z}_q$

commit



perfect hiding

open



binding under DL assumption

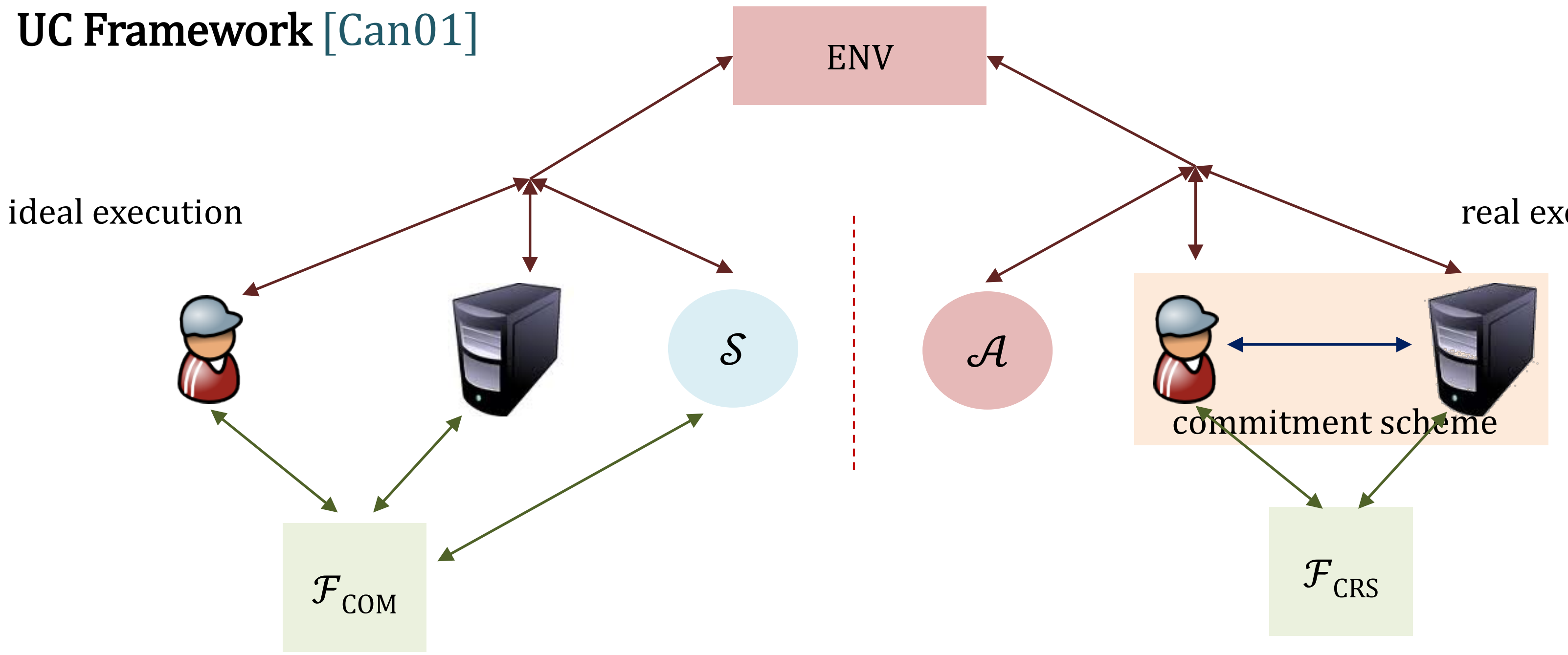
communication complexity one element of $\mathbb{G}$, one element of $\mathbb{Z}_q$

$\approx$ 512 bits for 128-bit security if $\mathbb{G} \subset E(\mathbb{F}_p)$

both stages are **non-interactive**

Universally Composable Commitments

UC Framework [Can01]



Commitment scheme is UC-secure if

for any $\mathcal{A}$ <u>there exists $\mathcal{S}$</u> such that

no ENV can tell ideal and real execution apart

Inevitable set-up assumption

UC-secure commitments require set-up [CF01]

e.g. *Common Reference String (CRS)*

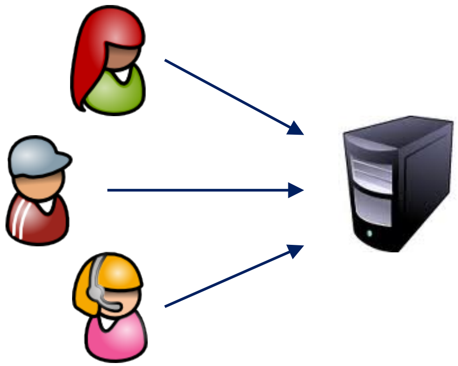
“Quality Criteria” for UC Commitments

Efficiency

communication complexity	# of bits communicated in both phases, ideally O(λ) <u>includes length of c and d</u>
computational complexity	total amount of work (often measured in pk ops)
length of the CRS	invariant in the # of message bits and users

CRS-reusability CRS should be re-usable for polynomially many commitments

Interactivity UC commitments should be non-interactive in both stages



main countermeasure against DoS attacks
e.g. in concurrent sessions or in more complex protocols

"Quality Criteria" for UC Commitments

Adaptive Security

UC commitments should resist adaptive corruptions

adaptive corruptions reveal the entire state of a party and can happen at any time

especially important for commitments due to the two-stage process

Secure erasures

UC commitments should not rely on secure erasures

often required to achieve adaptive security (e.g. erasure of ephemeral secrets)

can be realized using erasable memory [DFIJ99] or with trusted hardware assumption

Hardness Assumptions

ideally UC commitments should rely on weaker, more natural assumptions

10th Anniversary of UC Commitments

	UC scheme (CRS model)	CRS re-use	non-inter. stages	without erasures	adaptive security	hardness assumptions	
bit commitments	CF01 (1)	✘	✔	✔	✔	TDP	
	CF01 (2)	✔	✔	✘	✔	CFP + CCA PKE	
	CF01 (3)	✔	✔	✔	✔	DDH + UOWHF	
	CLOS02	✔	✔	✔	✔	TDP	
string commitments	DN02 (1)	✔	✘	✔	✔	p-subgroup	fact.
	DN02 (2)	✔	✘	✔	✔	DCR	
	DG03	✔	✘	✔	✔	DCR + Strong RSA	
	CS03	✔	✘	✘	✔	DCR + CHRF	
	NFT09	✘	✔	✘	✔	DCR + sEUF-OT	
	NFT09	✘	✔	✘	✔	DDH + sEUF-OT	dlog
	Lin11 (1)	✔	✘	✔	✘	DDH + CRHF	
	Lin11 (2)	✔	✘	✘	✔	DDH + CRHF	
tweaks	Our Scheme I	✔	✔	✘	✔	DLIN + CRHF	pairings
	Our Scheme II	✔	✔	✘	✔	DLIN + CRHF	

Ideal Functionality for Multiple Commitments

$\mathcal{F}_{\mathrm{MCOM}}$ as in [CF01] but with publicly delayed messages as in [HMQ04] :

high-level description

on **(commit, sid, cid, P_i, P_j, M)**

record (sid, cid, P_i, P_j, M)

publicly delayed output (receipt, sid, cid, P_i, P_j) to P_j

ignore any further input (commit, sid, cid, P_i, P_j, *)

on **(open, sid, cid, P_i, P_j)**

if recorded then publicly delayed output (open, sid, cid, P_i, P_j, M) to P_j

on **(corrupt-committer, sid, cid)**

if (sid, cid, P_i, P_j, M) is recorded then send M to the adversary $\mathcal{S}$

if $\mathcal{S}$ responds with M' then change the record to (sid, cid, P_i, P_j, M')

Lindell's Basic Scheme [Lin11]

CRS DL-hard group $\mathbb{G}$, generators g_1, g_2, random $c, d, h \in \mathbb{G}$, $h_1 = g_1^{\rho}$, $h_2 = g_2^{\rho}$

Cramer-Shoup PKE [CS98] with $pk_{CS} = (g_1, g_2, c, d, h)$ and CRHF H

Dual-Mode PKE [PVW08] with $pk_{DM} = (g_1, g_2, h_1, h_2)$ $(h_1, h_2) \approx (g_1^{\rho 1}, g_2^{\rho 2})$

alternative key for perfect hiding

(commit, sid, cid, P_i, P_j, M)

CRS
P_i

$x \leftarrow G(M, sid, cid, i, j)$ // reversible maping into $\mathbb{G}$

$c_{CS} = (u_1, u_2, e, w, v) \leftarrow CS.ENC(pk_{CS}, x; r)$

store r

c_{CS} →

CRS
P_j

(open, sid, cid, P_i, P_j)

CRS
P_i
r

M →

c_{CS} encrypts x

ZK proof

(pk_{DM} encrypts challenge)

CRS
P_j
c_{CS}

UC-secure against <u>static corruptions only</u>

- r must be stored until open stage
- for honest P_i : $\mathcal{S}$ encrypts 0
- for honest P_i : uses sk_{DM} to decrypt challenge
- for corrupted P_i : uses sk_{CS} to extract M

communication: $14 \cdot \lambda$ bits

<u>interactive</u> in the open phase

Generic Framework for Our First Scheme

CRS pk_{CCA} for IND-CCA secure PKE with labels (GEN, ENC, DEC)

crs_{NIZK} for simulation-sound NIZK$[M : c_{CCA} = Enc(pk_{CCA}, M, L; r)]$

(commit, sid, cid, P_i, P_j, M)

CRS P_i

label $L = P_i||sid||cid$

$c_{CCA} \leftarrow ENC(pk_{CCA}, M, L; r)$

$\pi_{CCA} \leftarrow NIZK[c_{CCA}$ encrypts $M](crs_{NIZK}, pk_{CCA}, M, L, r)$ — c_{CCA} → CRS P_j

erase ephemeral state except for π_{CCA}

(open, sid, cid, P_i, P_j)

CRS P_i — M, π_{CCA} → verify π_{CCA} CRS P_j L, c_{CCA}

UC-secure against adaptive corruptions

- $\mathcal{S}$ prepares crs_{NIZK} for simulation
- for honest P_i : $\mathcal{S}$ encrypts random R
- for honest P_i : simulates π_{CCA}
- for corrupted P_i : uses sk_{CCA} to extract M

non-interactive in both phases

Building Block 1

Groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order q with bilinear map $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$, $g, g_1, g_2 \in \mathbb{G}$

DLIN version of Cramer-Shoup PKE with labels [Sha07, HK07]

pk_{CS} : $X_1 = g_1^{x1}g^x$, $X_2 = g_2^{x2}g^x$, $X_3 = g_1^{x3}g^y$, $X_4 = g_2^{x4}g^y$, $X_5 = g_1^{x5}g^z$, $X_6 = g_2^{x6}g^z$

CRHF H

Encrypt

$$c_{CS} = (U_1, U_2, U_3, U_4, U_5)$$
$$= (g_1^{r}, g_2^{s}, g^{r+s}, M\cdot X_5^rX_6^s, (X_1X_3^{\alpha})^r\cdot(X_2X_4^{\alpha})^s)$$

with $\alpha = H(U_1, U_2, U_3, U_4, L)$ for some label L

Decrypt

check validity $U_5 \stackrel{?}{=} U_1^{x1+\alpha x3}U_2^{x2+\alpha x3}U_3^{x+\alpha y}$

if valid return $M = U_4/U_1^{x5}U_2^{x6}U_3^{z}$

IND-CCA secure under DLIN assumption : $(g^a, g^b, g^{ac}, g^{bd}, g^{c+d}) \approx (g^a, g^b, g^{ac}, g^{bd}, g^r)$

Building Block 2

Groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order q with bilinear map $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$

Groth-Sahai Proofs (for Multi-Exponentiation Equations) [GS08]

CRS $g, g_1, g_2 \in \mathbb{G}$, vectors $\mathbf{g_1} = (g_1, 1, g)$, $\mathbf{g_2} = (1, g_2, g)$, $\mathbf{g_3} \in \mathbb{G}^3$

Commit to $x \in \mathbb{Z}_q$: $c = ((1, 1, g)\cdot\mathbf{g_3})^x\cdot\mathbf{g_1}^r\cdot\mathbf{g_2}^s$

NIWI/NIZK proofs for equations of the form $\prod_{i=1}^{m} A_i^{y_i} \cdot \prod_{j=1}^{n} X_j^{b_j} \cdot \prod_{i=1}^{m}\cdot\prod_{j=1}^{n} X_j^{y_i c_{ij}} = T$

- if $\mathbf{g_3} = \mathbf{g_1}^{\xi_1}\cdot\mathbf{g_2}^{\xi_2}$ then c has perfect binding $\Rightarrow$ soundness setting for GS proofs
- if $\mathbf{g_3} = \mathbf{g_1}^{\xi_1}\cdot\mathbf{g_2}^{\xi_2} / (1, 1, g)$ then c has perfect hiding $\Rightarrow$ WI setting for GS proofs
  in this case (ξ_1, ξ_2) can be used to simulate NIWI/NIZK proofs
- under DLIN assumption the two values for $\mathbf{g_3}$ remain indistinguishable

Scheme I: Our Tweak on [Lin11]

CRS $g_1 = g^{\alpha_1}$, $g_2 = g^{\alpha_2}$, vectors $\mathbf{g_1} = (g_1, 1, g)$, $\mathbf{g_2} = (1, g_2, g)$, $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2}$
DLIN Cramer-Shoup PKE $pk_{CS} = (X_1, \ldots, X_6)$, CRHF $H : \{0,1\} \longrightarrow \mathbb{Z}_q$

(commit, sid, cid, P_i, P_j, M) with $M \in \mathbb{G}$

CRS
P_i

label $L = P_i || sid || cid$
$c_{CS} = (U_1, U_2, U_3, U_4, U_5) \leftarrow CS.ENC(pk_{CS}, M, L; r, s)$
$\pi_{CS} \leftarrow GSNIZK[c_{CS}$ encrypts $M]$
erase ephemeral state except for π_{CS}

c_{CS} →

CRS
P_j

(open, sid, cid, P_i, P_j)

CRS
P_i

M, π_{CS} →

verify π_{CS}

CRS
P_j
L, c_{CS}

UC-secure against adaptive corruptions

- $\mathcal{S}$ sets $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2} / (1, 1, g)$ - WI setting
- for honest P_i : $\mathcal{S}$ encrypts random R
- for honest P_i : uses (ξ_1, ξ_2) to simulate π_{CS}
- for corrupted P_i : uses sk_{CS} to extract M

communication: 21 elements of $\mathbb{G}$
non-interactive in both phases

Camenisch-Shoup UC Commitments [CS03]

CRS group $\mathbb{G}_n \subset \mathbb{Z}^*_{n^2}$, safe RSA modulus n, generators g, h of $\mathbb{G}_n$

[Ped91] $pk_{Ped} = (\gamma_1, \gamma_2)$, Verifiable PKE [CS03] $pk_{VE} = (n, g, y_1, y_2, y_3)$

(commit, sid, cid, P_i, P_j, M) with $M \in \mathbb{Z}_n$

CRS
P_i

$c_{Ped} = \gamma_1^M \gamma_2^r$
label $L = P_i || sid || cid$
$c_{VE} = (u, e, v) \leftarrow VE.ENC(pk_{VE}, (M, r), L; s)$
erase ephemeral state except r

c_{Ped}, c_{VE} →

c_{VE} encrypts representation of c_{Ped}

ZK proof

CRS
P_j

(open, sid, cid, P_i, P_j)

CRS
P_i
r

M, r →

CRS
P_j
c_{Ped}

UC-secure against <u>adaptive corruptions</u>

- $\mathcal{S}$ knows $\log_{\gamma_1}(\gamma_2)$
- for honest P_i : $\mathcal{S}$ encrypts 0
- for corrupted P_i : uses sk_{VE} to extract M

communication: $94 \cdot \lambda$ bits

<u>interactive</u> in the commit phase

Building Block 3

in addition to DLIN-based Cramer-Shoup PKE and Groth-Sahai framework

Trapdoor commitments by Cathalo, Libert, and Yung [CLY09]

CRS vectors $\mathbf{f_1} = (f_1, 1, g)$, $\mathbf{f_2} = (1, f_2, g)$, $\mathbf{f_3} = \mathbf{f_1}^{x1} \cdot \mathbf{f_2}^{x2} \cdot (1, 1, g)^{x3}$, $f_1, f_2, g \in \mathbb{G}$

Trapdoor (x_1, x_2, x_3)

Commit to $X \in \mathbb{G}$: $c = (c_1, c_2, c_3) = (1, 1, X) \cdot \mathbf{f_1}^{\alpha} \cdot \mathbf{f_2}^{\beta} \cdot \mathbf{f_3}^{\gamma}$

Open: publish $(g^{\alpha}, g^{\beta}, g^{\gamma})$

Verify:
$$e(c_1, g) = e(f_1, g^{\alpha}) \cdot e(f_{3,1}, g^{\gamma})$$
$$e(c_2, g) = e(f_2, g^{\beta}) \cdot e(f_{3,2}, g^{\gamma})$$
$$e(c_3, g) = e(X \cdot g^{\alpha} \cdot g^{\beta}, g) \cdot e(f_{3,3}, g^{\gamma})$$

- if $x_3 \neq 0$ then c has perfect hiding and DLIN-based binding
- if $x_3 \neq 0$ then c can be equivocated using the trapdoor (x_1, x_2, x_3)
- if $x_3 = 0$ then c has perfect binding
- if $x_3 = 0$ and $dlog_g(f_1)$ and $dlog_g(f_2)$ are known then c becomes extractable

Scheme II: Our Tweak on [CS03]

CRS $g_1 = g^{\alpha 1}$, $g_2 = g^{\alpha 2}$, vectors $\mathbf{g_1} = (g_1, 1, g)$, $\mathbf{g_2} = (1, g_2, g)$, $\mathbf{g_3} = \mathbf{g_1}^{\xi 1} \cdot \mathbf{g_2}^{\xi 2}$

[CLY09] $f_1, f_2 \in \mathbb{G}$, vectors $\mathbf{f_1} = (f_1, 1, g)$, $\mathbf{f_2} = (1, f_2, g)$, $\mathbf{f_3} = \mathbf{f_1}^{x1} \cdot \mathbf{f_2}^{x2} \cdot (1, 1, g)^{x3}$

DLIN Cramer-Shoup PKE $pk_{CS} = (X_1, \ldots, X_6)$, CRHF $H : \{0,1\} \longrightarrow \mathbb{Z}_q$

(commit, sid, cid, P_i, P_j, M) with $M \in \mathbb{G}$

CRS P_i

$c_{CLY} = (1, 1, M) \cdot \mathbf{f_1}^{\alpha} \cdot \mathbf{f_2}^{\beta} \cdot \mathbf{f_3}^{\gamma}$

label $L = P_i || sid || cid$

$c_{CS} = (U_1, U_2, U_3, U_4, U_5) \leftarrow CS.ENC(pk_{CS}, M, L; r, s)$

$\pi_{CS} \leftarrow$ GSNIZK[c_{CS} is a valid ciphertext]

$\pi_{CLY} \leftarrow$ GSNIZK[consistency of c_{CS} and c_{CLY}]

erase ephemeral state except for $(g^{\alpha}, g^{\beta}, g^{\gamma})$

$c_{CLY}, c_{CS}, \pi_{CS}, \pi_{CLY}$ →

CRS P_j

verify π_{CS}, π_{CLY}

UC-secure against <u>adaptive corruptions</u>

- $\mathcal{S}$ sets $\mathbf{g_3} = \mathbf{g_1}^{\xi 1} \cdot \mathbf{g_2}^{\xi 2} / (1, 1, g)$ - perfect hiding
- for honest P_i : $\mathcal{S}$ commits to R and encrypts R
- for honest P_i : uses (x_1, x_2, x_3) to equivocate c_{CLY}
- for corrupted P_i : uses sk_{CS} to extract M

communication: $40 \cdot \lambda$ bits

<u>non-interactive</u> in both phases

(open, sid, cid, P_i, P_j)

CRS P_i

$M, (g^{\alpha}, g^{\beta}, g^{\gamma})$ →

verify c_{CLY}

CRS P_j

L, c_{CLY}

10th Anniversary of UC Commitments

UC scheme (CRS model)	CRS re-use	non-inter. stages	without erasures	adaptive security	communication complexity (bits)
CF01 (1)	✗	✓	✓	✓	$O(\ell \cdot \lambda)$
CF01 (2)	✓	✓	✗	✓	$O(\ell \cdot \lambda)$
CF01 (3)	✓	✓	✓	✓	$O(\ell \cdot \lambda)$
CLOS02	✓	✓	✓	✓	$O(\ell \cdot \lambda)$
DN02 (1)	✓	✗	✓	✓	$18 \cdot \lambda$ (13824)
DN02 (2)	✓	✗	✓	✓	$24 \cdot \lambda$ (18432)
DG03	✓	✗	✓	✓	$16 \cdot \lambda$ (12288)
CS03	✓	✗	✗	✓	**$94 \cdot \lambda$ (72192)**
NFT09	✗	✓	✗	✓	$21 \cdot \lambda$ (16128)
NFT09	✗	✓	✗	✓	$O(\ell \cdot \lambda)$
Lin11 (1)	✓	✗	✓	✗	$14 \cdot \lambda$ (3584)
Lin11 (2)	✓	✗	✗	✓	**$19 \cdot \lambda$ (4864)**
Our Scheme I	✓	✓	✗	✓	**$5 \cdot \lambda + 16 \cdot \lambda$ (5376)**
Our Scheme II	✓	✓	✗	✓	**$37 \cdot \lambda + 3 \cdot \lambda$ (10240)**

λ sec. par.
$\ell = |M|$ bits

$\lambda = 768$ bits
$\ell \leq \lambda$

$\lambda = 256$ bits
$\ell \leq \lambda$

$\lambda = 256$ bits
$\ell \leq \lambda$

Open Challenges

UC scheme (CRS)	CRS re-use	non-inter. stages	without erasures	adaptive security	communication complexity (bits)
this work	✓	✓	✗	✓	$21 \cdot \lambda$ (5376)
????	✓	✓	✓	✓	????

in CRS model
w/o stronger assumptions

reduce comm. compl.
recall [Ped91] $2 \cdot \lambda$ (512)