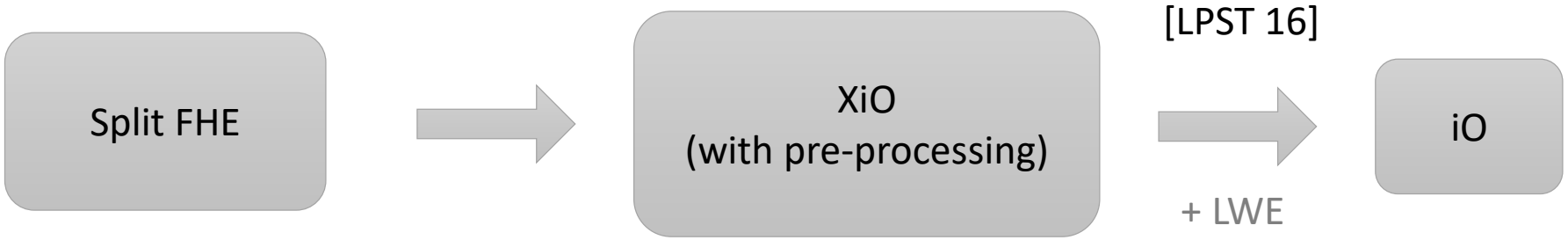
Circularity-based iO: part 2

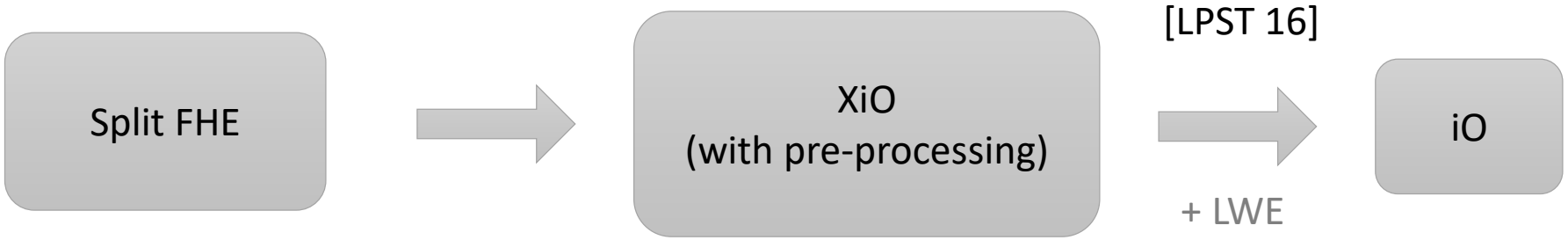
Romain Gay – IBM Research Zürich

Joint work with Rafael Pass – Cornell Tech

Recap



Recap



$FHE(\vec{m})$

$\downarrow f$

$FHE(f(\vec{m}))$

$\downarrow \rho_f$: Succinct
Reveal only $f(\vec{m})$

$f(\vec{m})$

Our Result

iO from:

- LWE
- strong CIRC conjecture w.r.t. standard LWE-based encryptions

Circular Security

[Camenisch Lysyanskaya 01, Black Rogaway Shrimpton 02,…]

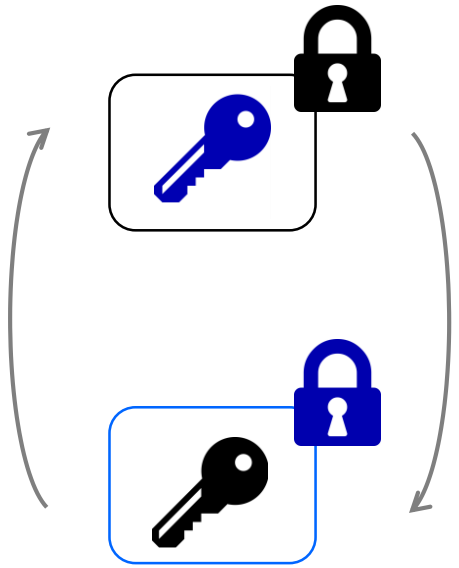
PKE: 

pk sk

$\overline{\text{PKE}}$: 

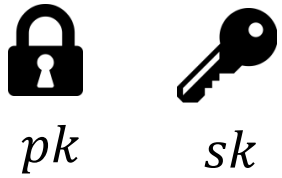
$\overline{pk}$ $\overline{sk}$

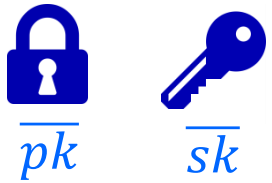
Security is preserved with:

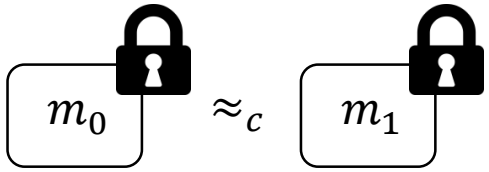


Circular Security

[Camenisch Lysyanskaya 01, Black Rogaway Shrimpton 02,…]

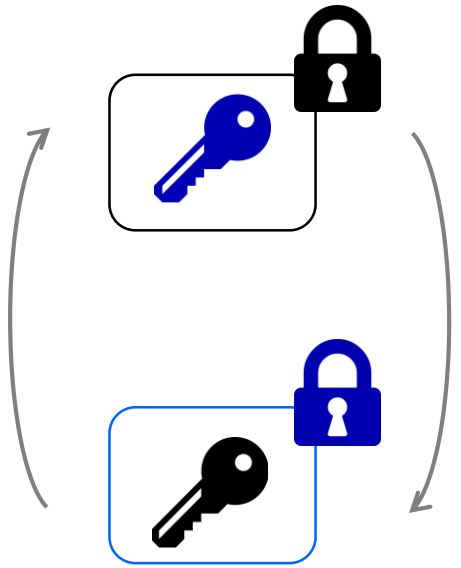
PKE: 

$\overline{\text{PKE}}$: 



Semantic security

preserved with:



CIRC conjecture: for “natural” schemes, semantic security is preserved in the presence of an encrypted key cycle.

Circular Security

[Camenisch Lysyanskaya 01, Black Rogaway Shrimpton 02,…]

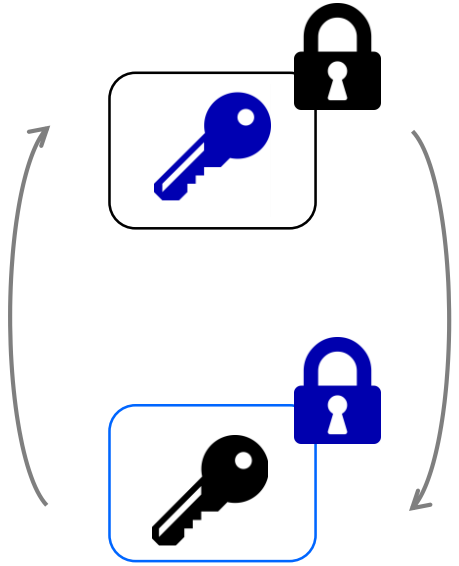
PKE: pk sk

$\overline{\text{PKE}}$: $\overline{pk}$ $\overline{sk}$

$m_0 \approx_c m_1$

Semantic security

preserved with:



CIRC conjecture: for “natural” schemes, semantic security is preserved in the presence of an encrypted key cycle.

Application: Bootstrapping for unlevelled FHE [Gentry 09]

Circular Security

[Camenisch Lysyanskaya 01, Black Rogaway Shrimpton 02,…]

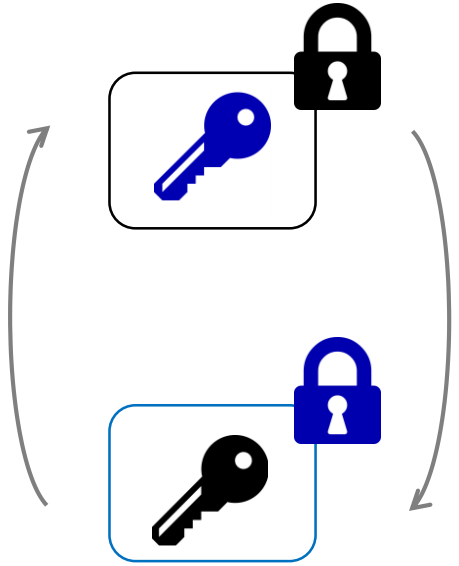
PKE: pk sk

$\overline{\text{PKE}}$: $\overline{pk}$ $\overline{sk}$

$m_0 \approx_c m_1$

Semantic security

preserved with:



CIRC conjecture: for “natural” schemes, semantic security is preserved in the presence of an encrypted key cycle.

strong CIRC conjecture: for “natural” schemes & “natural” XXX security, XXX security is preserved in the presence of an encrypted key cycle

XXX=CCA, leakage resilient,…

Our Result

iO from*:
- LWE
- strong CIRC conjecture

w.r.t: XXX security = Shielded Randomness Leakage (SRL) security

PKE: Gentry, Sahai, Waters (GSW) FHE

$\overline{\mathrm{PKE}}$: Packed-Regev encryption

*subexponential hardness of the underlying assumptions is required

Our Result

iO from*:
- LWE
- strong CIRC conjecture

w.r.t: XXX security = Shielded Randomness Leakage (SRL) security

PKE: Gentry, Sahai, Waters (GSW) FHE

$\overline{\mathrm{PKE}}$: Packed-Regev encryption

Thm 1: LWE ⇒ GSW is SRL secure

*subexponential hardness of the underlying assumptions is required

Our Result

iO from*:
- LWE
- strong CIRC conjecture

w.r.t: XXX security = Shielded Randomness Leakage (SRL) security

PKE: Gentry, Sahai, Waters (GSW) FHE

$\overline{\mathrm{PKE}}$: Packed-Regev encryption

Thm 1: LWE ⇒ GSW is SRL secure

Thm 2: LWE + SRL security of GSW is preserved in the presence of a (GSW,P-Regev) key cycle ⇒ iO

*subexponential hardness of the underlying assumptions is required

SRL Security

$FHE(m_1; r_1), \dots, FHE(m_n; r_n)$

Homomorphic evaluation of f

$FHE(f(m_1, \dots, m_n); r_f)$

Randomness homomorphism

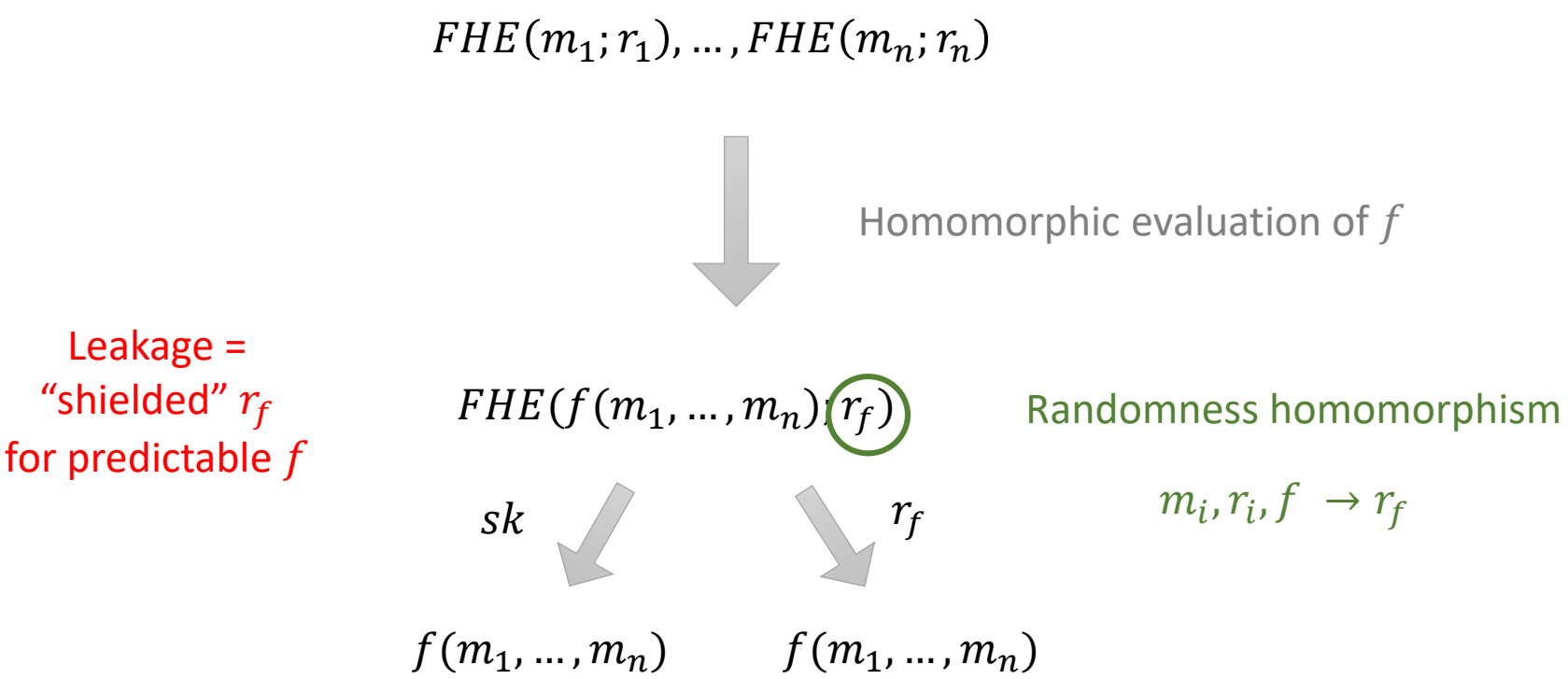
$m_i, r_i, f \rightarrow r_f$

sk

r_f

$f(m_1, \dots, m_n)$ $f(m_1, \dots, m_n)$

SRL Security



SRL Security

$$FHE(m_1; r_1), \ldots, FHE(m_n; r_n) = FHE(\vec{m}; \vec{r})$$

Homomorphic evaluation of f

Leakage =
"shielded" r_f
for predictable f

$$FHE(f(\vec{m}); r_f)$$

Randomness homomorphism

$$\vec{m}, \vec{r}, f \rightarrow r_f$$

sk $\qquad$ r_f

$f(\vec{m})$ $\qquad$ $f(\vec{m})$

SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b; \vec{r})$

Challenger

$b \leftarrow_R \{0,1\}$

SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b; \vec{r})$

Challenger

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

(f, α)

leak

b'

$r^\star \leftarrow_R$ fresh

If $f(\vec{m}_b) = \alpha$, leak $= r_f + r^\star$

Otherwise, leak $= \perp$ and Adversary FAILS

SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

Challenger

$FHE(\vec{m}_b; \vec{r})$

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

$r^\star \leftarrow_R$ fresh

(f, α)

If $f(\vec{m}_b) = \alpha$, leak $= r_f + r^\star$

leak

Otherwise, leak $= \perp$ and Adversary FAILS

b'

Win: $b' = b$ and valid queries

SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b; \vec{r})$

Challenger

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

(f, α)

leak

b'

$r^\star \leftarrow_R$ fresh

If $f(\vec{m}_b) = \alpha$, leak $= r_f + r^\star$

Otherwise, leak $= \perp$ and Adversary FAILS

Win: $b' = b$ and valid queries

SRL secure: Win $\leq \frac{1}{2} + negl$

SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b; \vec{r})$

Challenger

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

(f, α)

leak

b'

$r^\star \leftarrow_R$ fresh

If $f(\vec{m}_b) = \alpha$, leak $= r_f + r^\star$

Otherwise, leak $= \perp$ and Adversary FAILS

Win: $b' = b$ and valid queries

SRL secure: Win $\leq \frac{1}{2} + negl$

Thm 1: LWE ⇒ GSW is SRL secure

Circular SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b|\overline{sk}; \vec{r}), \overline{\text{PKE}}(sk)$

Challenger

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

(f, α)

leak

b'

$r^\star \leftarrow_R$ fresh

If $f(\vec{m}_b|\overline{sk}) = \alpha$, leak $= r_f + r^\star$

Otherwise, leak $= \perp$ and Adversary FAILS

Win: $b' = b$ and valid queries

SRL secure: Win $\leq \frac{1}{2} + negl$

Circular SRL Security

Adversary

pk

$(\vec{m}_0, \vec{m}_1)$

$FHE(\vec{m}_b|\overline{sk}; \vec{r}), \overline{\text{PKE}}(sk)$

Challenger

$b \leftarrow_R \{0,1\}$

$FHE(0; r^\star)$

(f, α)

leak

b'

$r^\star \leftarrow_R$ fresh

If $f(\vec{m}_b|\overline{sk}) = \alpha$, leak $= r_f + r^\star$

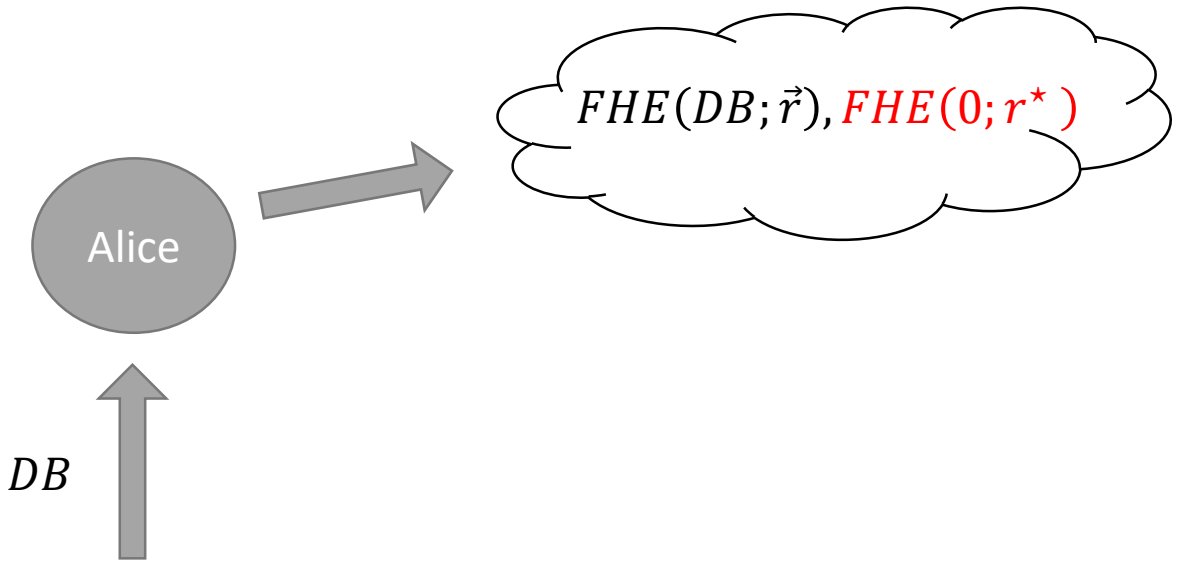
Otherwise, leak $= \perp$ and Adversary FAILS

Win: $b' = b$ and valid queries

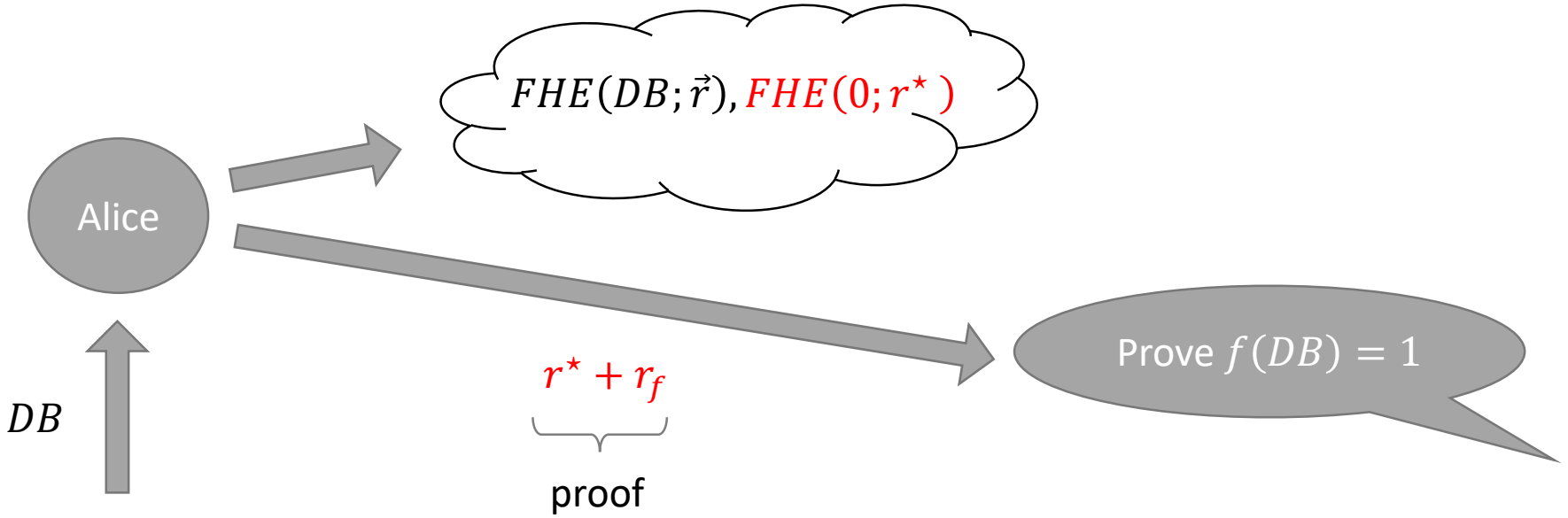
SRL secure: Win $\leq \frac{1}{2} + negl$

Thm 2: LWE & (GSW,P-Regev) are circular SRL secure ⇒ iO

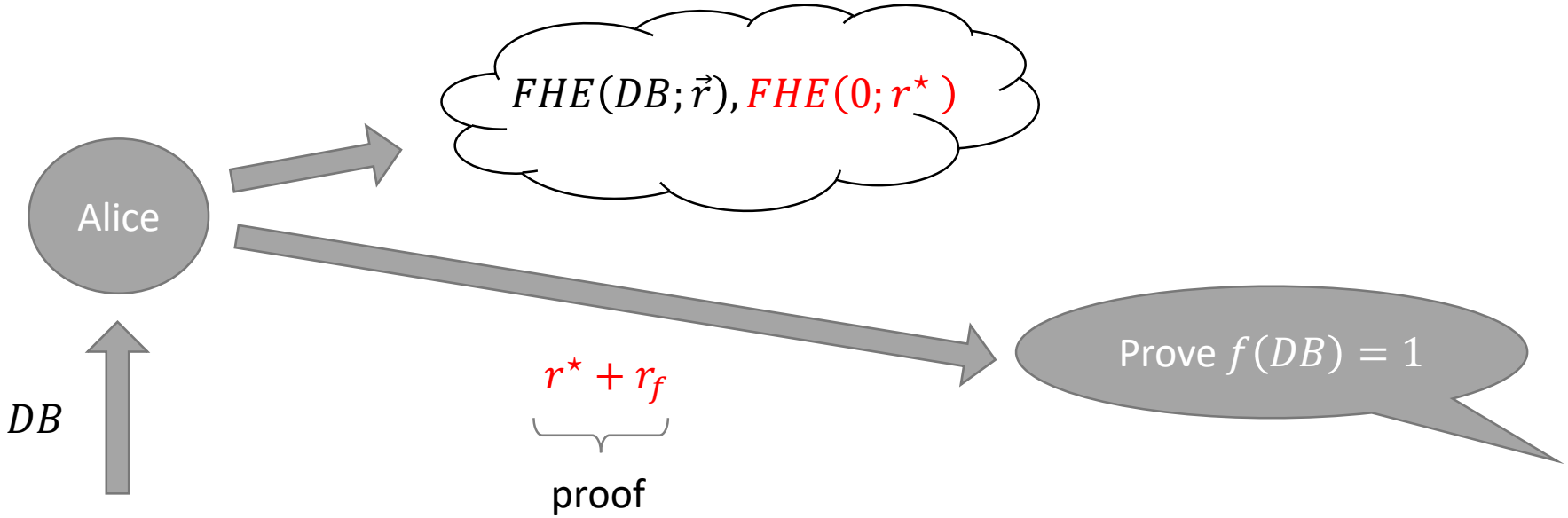
Application of (plain) SRL security



Application of (plain) SRL security



Application of (plain) SRL security



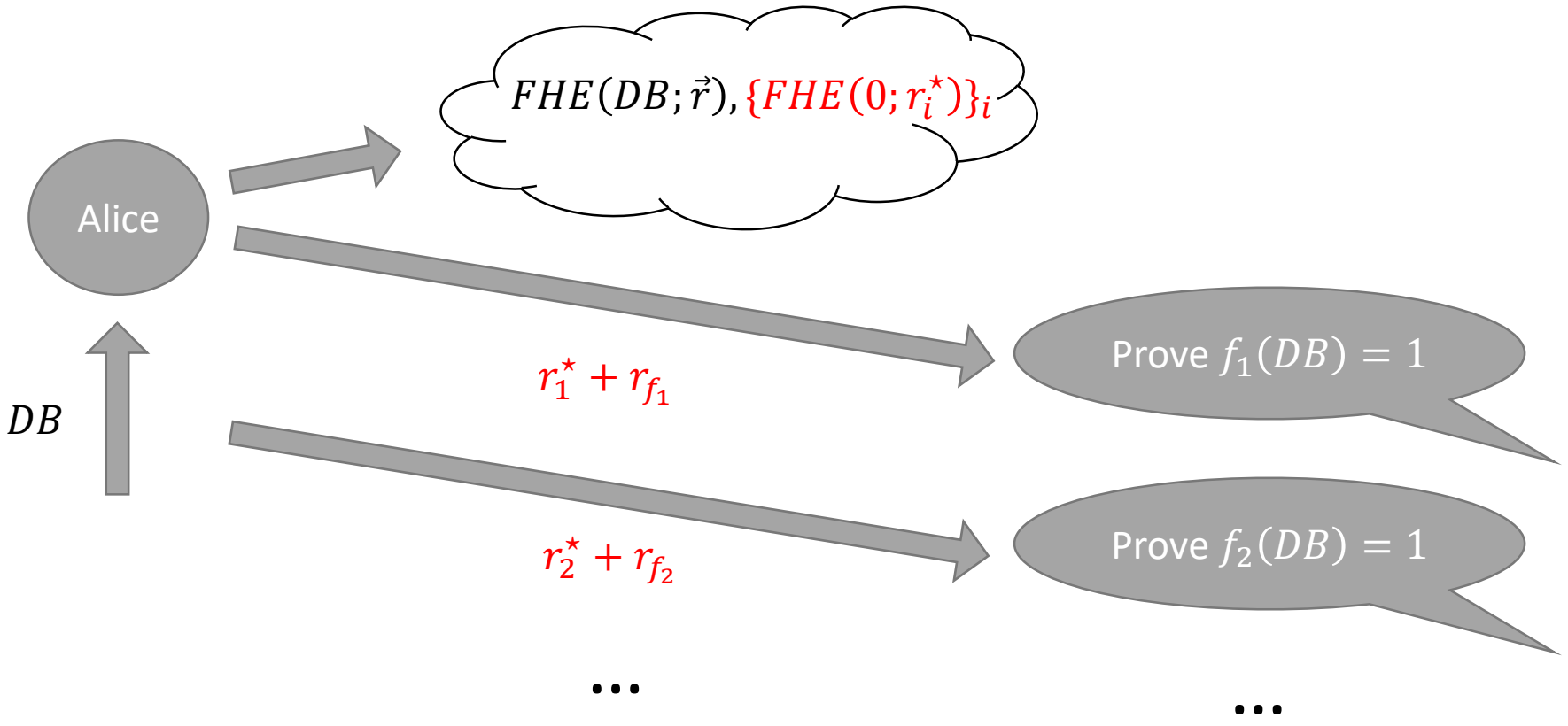
Verification: $FHE(DB;\vec{r})$ → Homomorphic evaluation of f → $FHE(f(DB);r_f)$

$+ \; FHE(0;r^\star)$ $=$ $FHE(f(DB);r^\star + r_f)$

↓ Open with $r^\star + r_f$

$f(DB)$

Application of (plain) SRL security



Our Result

iO from:
- LWE
- strong CIRC conjecture

w.r.t: XXX security = Shielded Randomness Leakage (SRL) security

PKE: Gentry, Sahai, Waters (GSW) FHE

$\overline{\mathrm{PKE}}$: Packed-Regev encryption

Thm 1: LWE ⇒ GSW is SRL secure

Thm 2: LWE + (GSW,P-Regev) are circular SRL secure ⇒ iO

Our Result

iO from:
- LWE
- strong CIRC conjecture

w.r.t: XXX security = Shielded Randomness Leakage (SRL) security

PKE: Gentry, Sahai, Waters (GSW) FHE

$\overline{\mathrm{PKE}}$: Packed-Regev encryption

Thm 1: LWE ⇒ GSW is SRL secure

Thm 2: LWE + (GSW,P-Regev) are circular SRL secure ⇒ iO

Recap: [BDGM20a] Split FHE

$$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk)$$

$\downarrow f$

$$FHE(f(\vec{m}))$$

$\downarrow$ Proxy re-encrypt

$$\overline{LHE}(f(\vec{m}) + noise_i)$$

Recap: [BDGM20a] Split FHE

$$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk)$$

f

$$FHE(f(\vec{m}))$$

Proxy re-encrypt

fresh

$$\overline{LHE}(f(\vec{m}) + noise_i) \quad + \quad \overline{LHE}(s_i)$$

$$= \quad \overline{LHE}(f(\vec{m}) + noise_i + s_i; \bar{r}_i)$$

Recap: [BDGM20a] Split FHE

$$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk)$$

f

$$FHE(f(\vec{m}))$$

Proxy re-encrypt

$$\overline{LHE}(f(\vec{m}) + noise_i)$$

fresh

$$\overline{LHE}(s_i)$$

$$\overline{LHE}(f(\vec{m}) + noise_i + s_i; \bar{r}_i)$$

Open with $\bar{r}_i$

$$f(\vec{m}) + noise_i + s_i$$

Recap: [BDGM20a] Split FHE

$$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk)$$

f

$$FHE(f(\vec{m}))$$

Proxy re-encrypt

$$\overline{LHE}(f(\vec{m}) + noise_i)$$

fresh

$$\overline{LHE}(s_i)$$

$$\overline{LHE}(f(\vec{m}) + noise_i + s_i; \bar{r}_i)$$

Open with $\bar{r}_i$

$$f(\vec{m}) + noise_i + s_i$$

Recap: [BDGM20a] Split FHE

$$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk), FHE(\overline{sk})$$

f

$$FHE(f(\vec{m}))$$

Proxy re-encrypt

$$\overline{LHE}(f(\vec{m}) + noise_i)$$

Dense $\overline{ct}$

$$\overline{LHE}(u_i)$$

Proxy re-encrypt & round

$$FHE(LSB(u_i))$$

Proxy re-encrypt

$$\overline{LHE}(LSB(u_i) + noise'_i)$$

Recap: [BDGM20a] Split FHE

Dense $\overline{ct}$

$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk), FHE(\overline{sk})$

$\overline{LHE}(u_i)$

f

Proxy re-encrypt & round

$FHE(f(\vec{m}))$

$FHE(LSB(u_i))$

Proxy re-encrypt

Proxy re-encrypt

$\overline{LHE}(f(\vec{m}) + noise_i)$ + $\overline{LHE}(LSB(u_i) + noise'_i)$

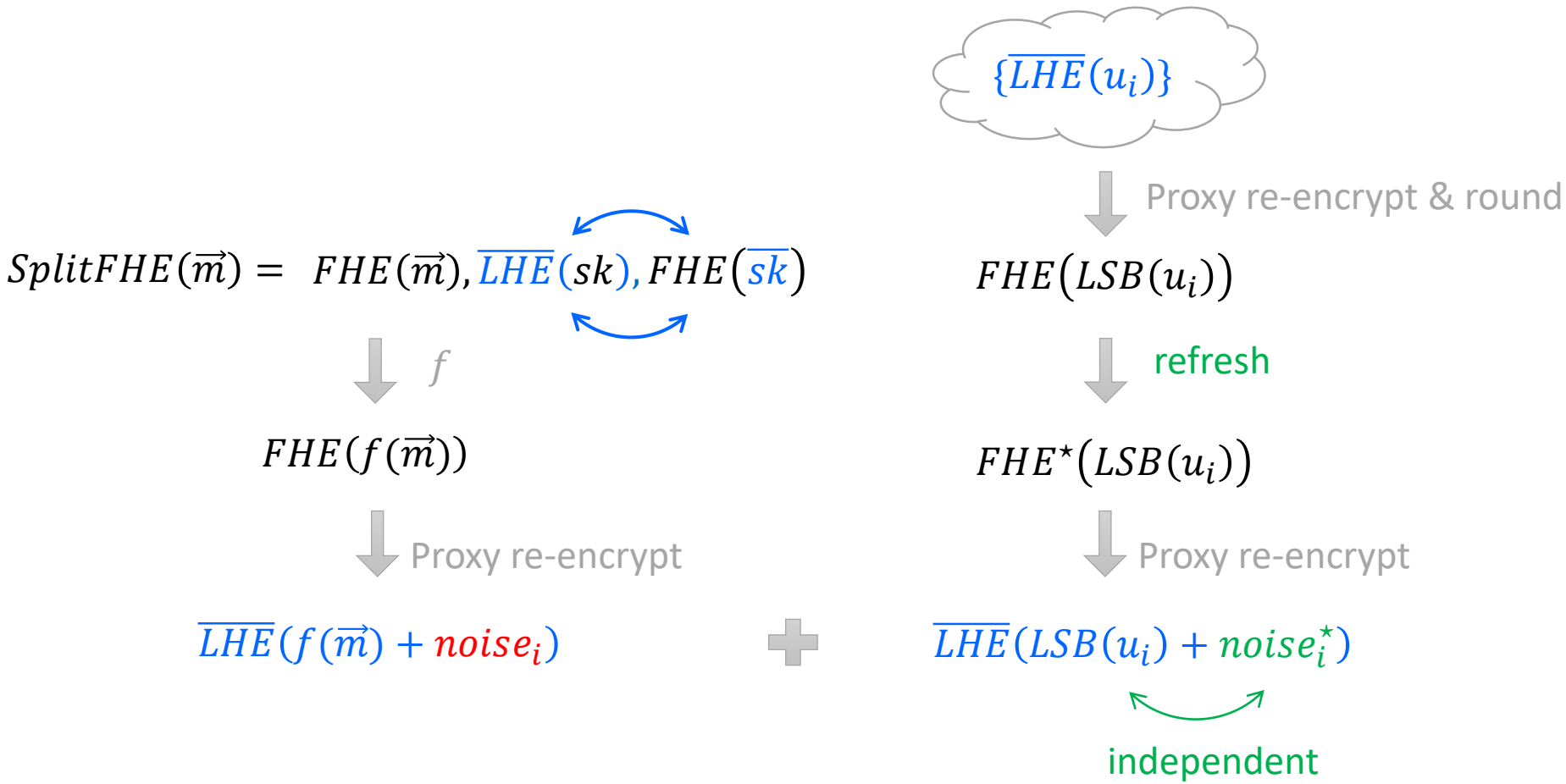
correlated

heuristically secure

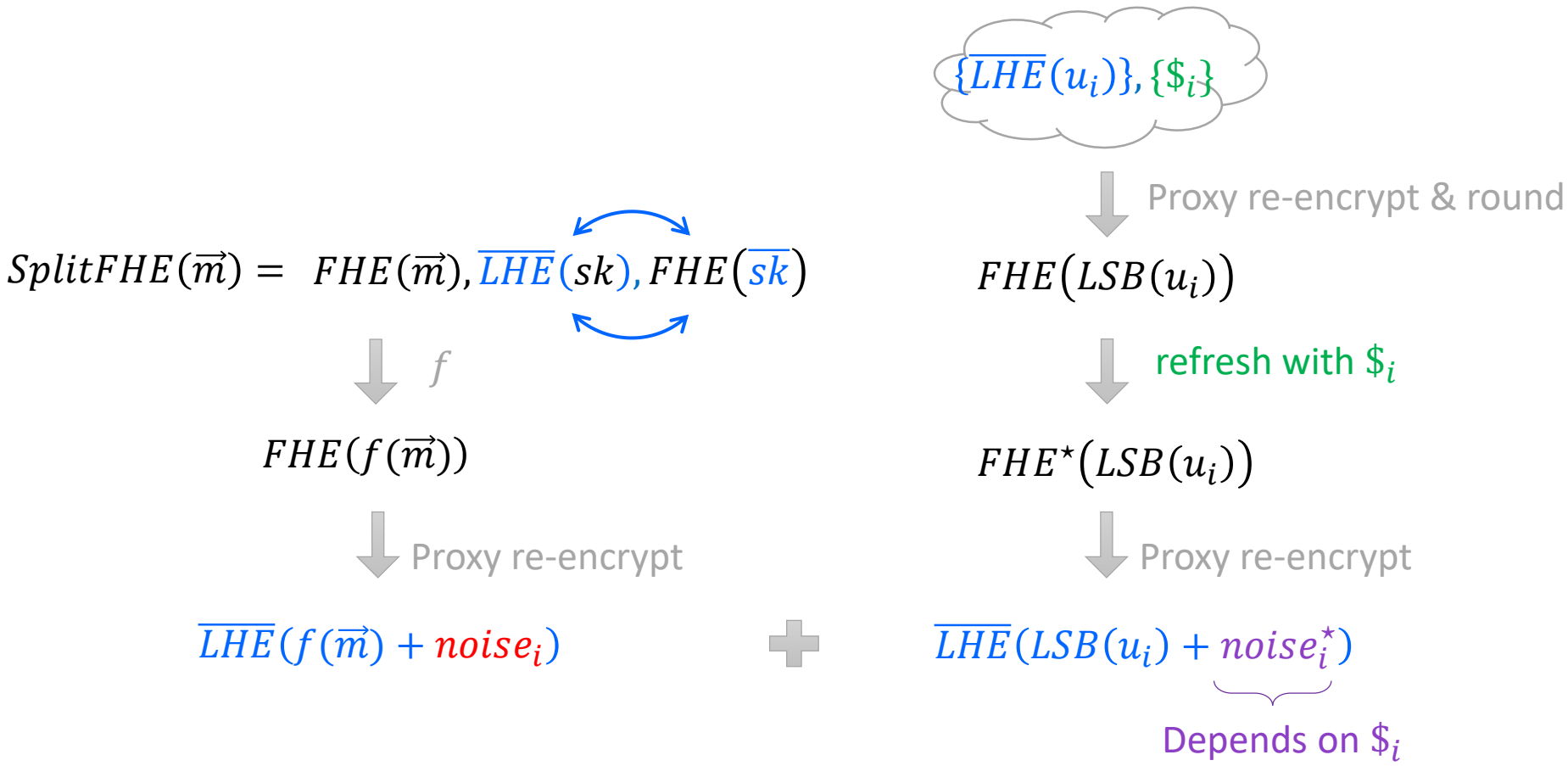
Our Result

- Replace RO by CRS (and rely on XiO with pre-processing)
- Refresh FHE eval to break correlations
  - Reveal random coins and use SRL security

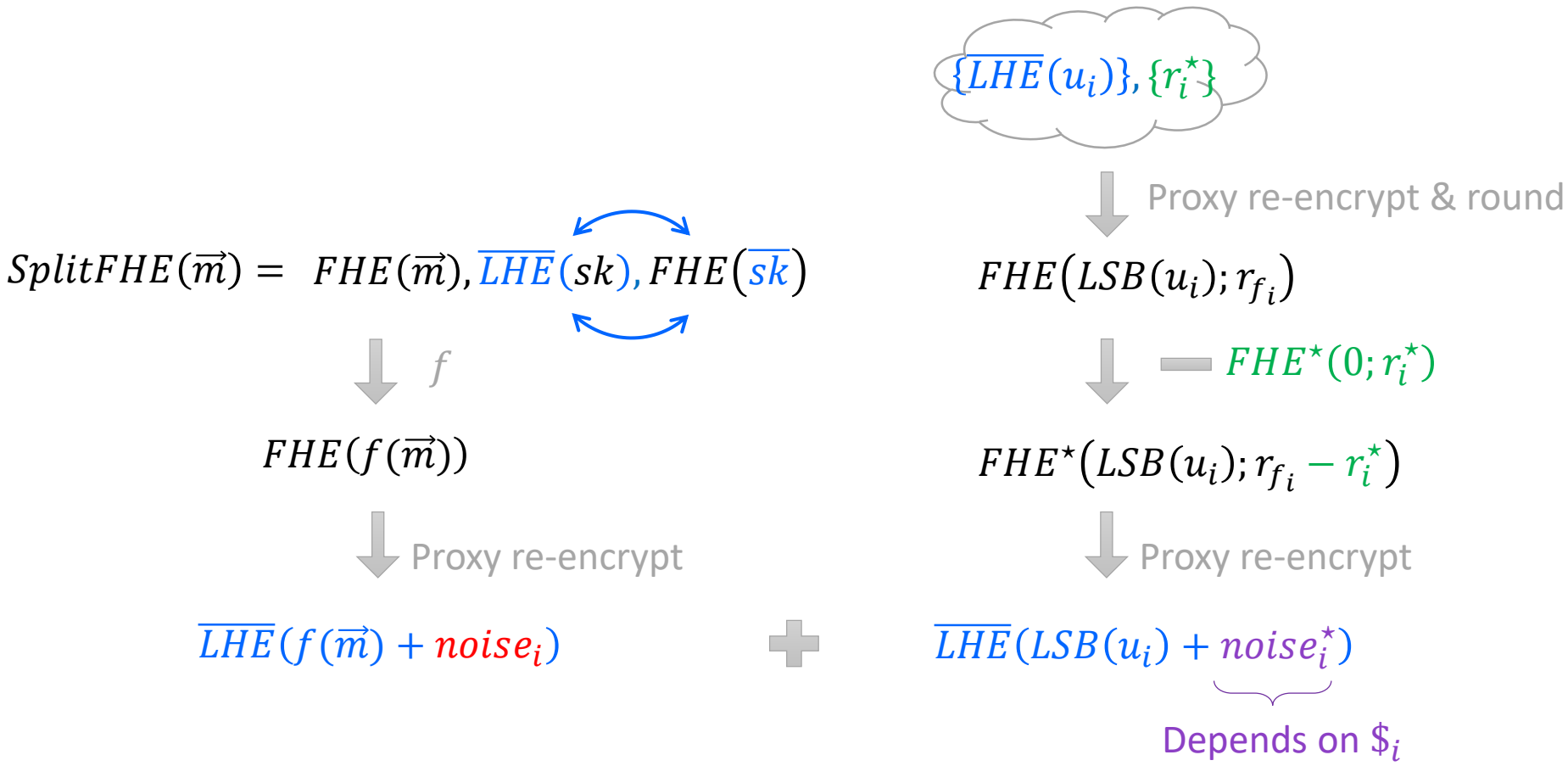
Our Result


$\{\overline{LHE}(u_i)\}$
Proxy re-encrypt & round
$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk), FHE(\overline{sk})$
f
refresh
$FHE(f(\vec{m}))$
$FHE(LSB(u_i))$
$FHE^{\star}(LSB(u_i))$
Proxy re-encrypt
Proxy re-encrypt
$\overline{LHE}(f(\vec{m}) + noise_i)$
$\overline{LHE}(LSB(u_i) + noise_i^{\star})$
independent

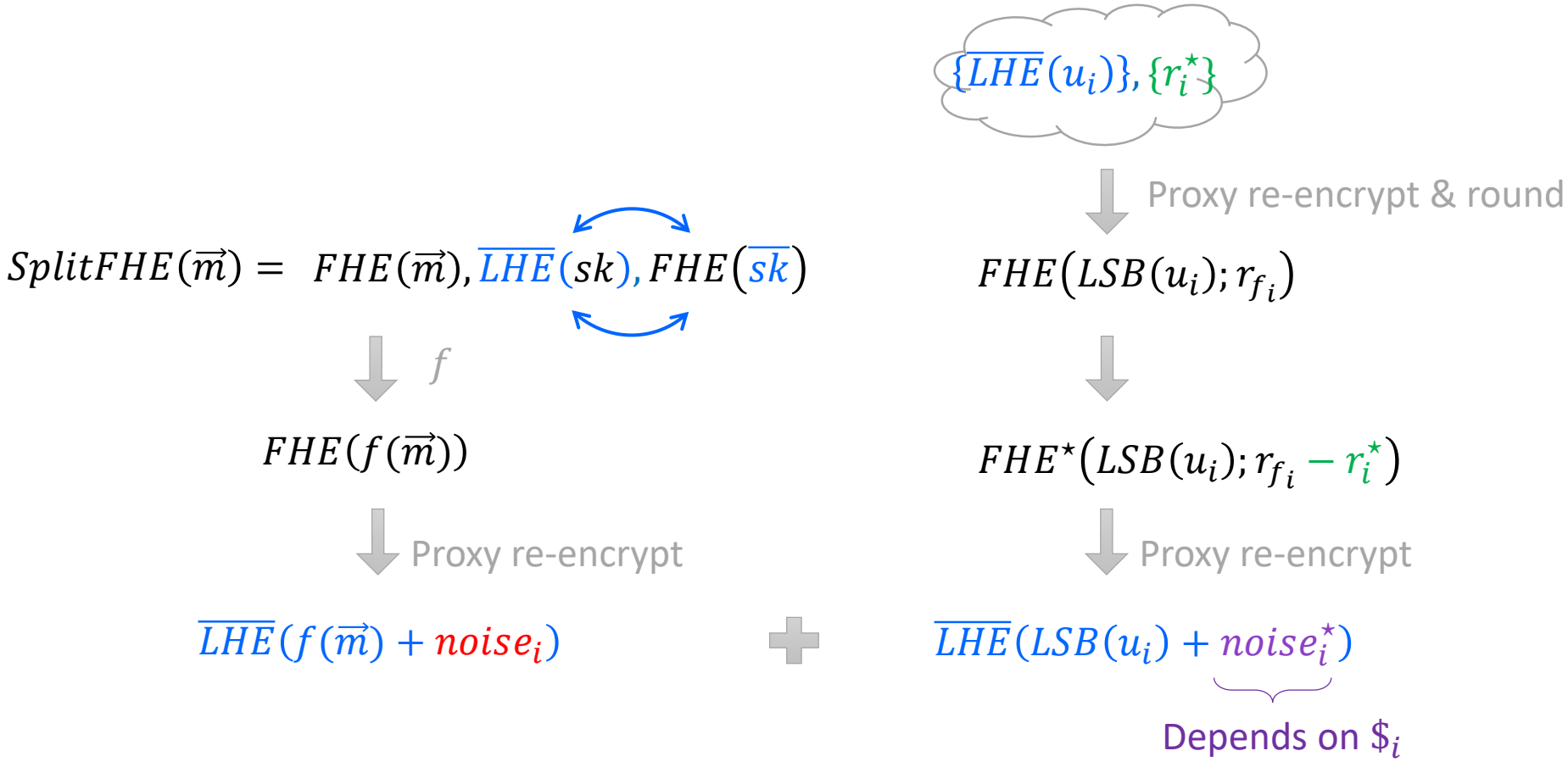
Our Result


$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk), FHE(\overline{sk})$
f
$FHE(f(\vec{m}))$
Proxy re-encrypt
$\overline{LHE}(f(\vec{m}) + noise_i)$
$\{\overline{LHE}(u_i)\}, \{\$_i\}$
Proxy re-encrypt & round
$FHE(LSB(u_i))$
refresh with $\$_i$
$FHE^{\star}(LSB(u_i))$
Proxy re-encrypt
$\overline{LHE}(LSB(u_i) + noise_i^{\star})$
Depends on $\$_i$

Our Result

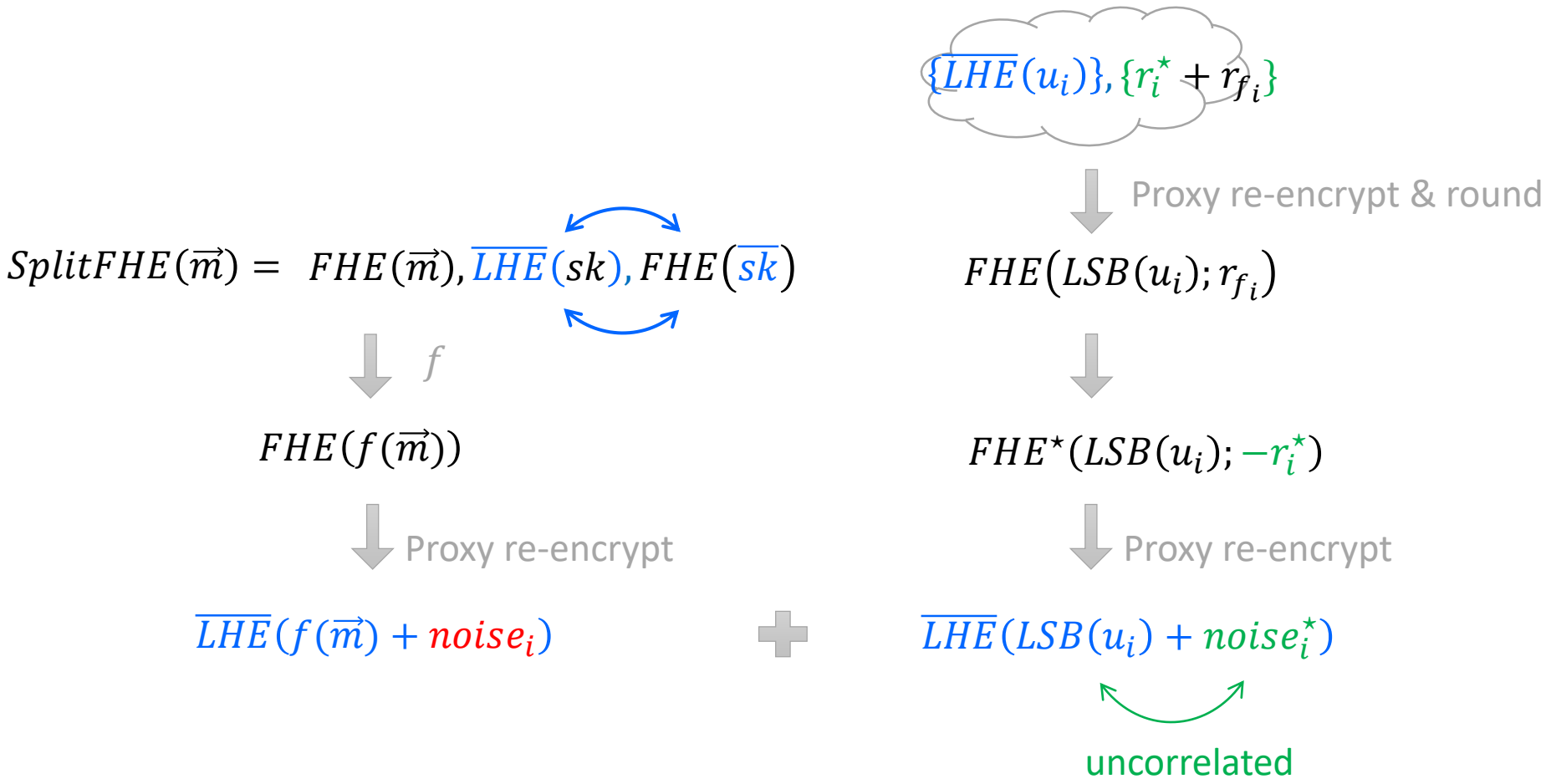

$SplitFHE(\vec{m}) = FHE(\vec{m}), \overline{LHE}(sk), FHE(\overline{sk})$
f
$FHE(f(\vec{m}))$
Proxy re-encrypt
$\overline{LHE}(f(\vec{m}) + noise_i)$
$\{\overline{LHE}(u_i)\}, \{r_i^\star\}$
Proxy re-encrypt & round
$FHE(LSB(u_i); r_{f_i})$
$FHE^\star(0; r_i^\star)$
$FHE^\star(LSB(u_i); r_{f_i} - r_i^\star)$
Proxy re-encrypt
$\overline{LHE}(LSB(u_i) + noise_i^\star)$
Depends on $\$_i$

Our Result



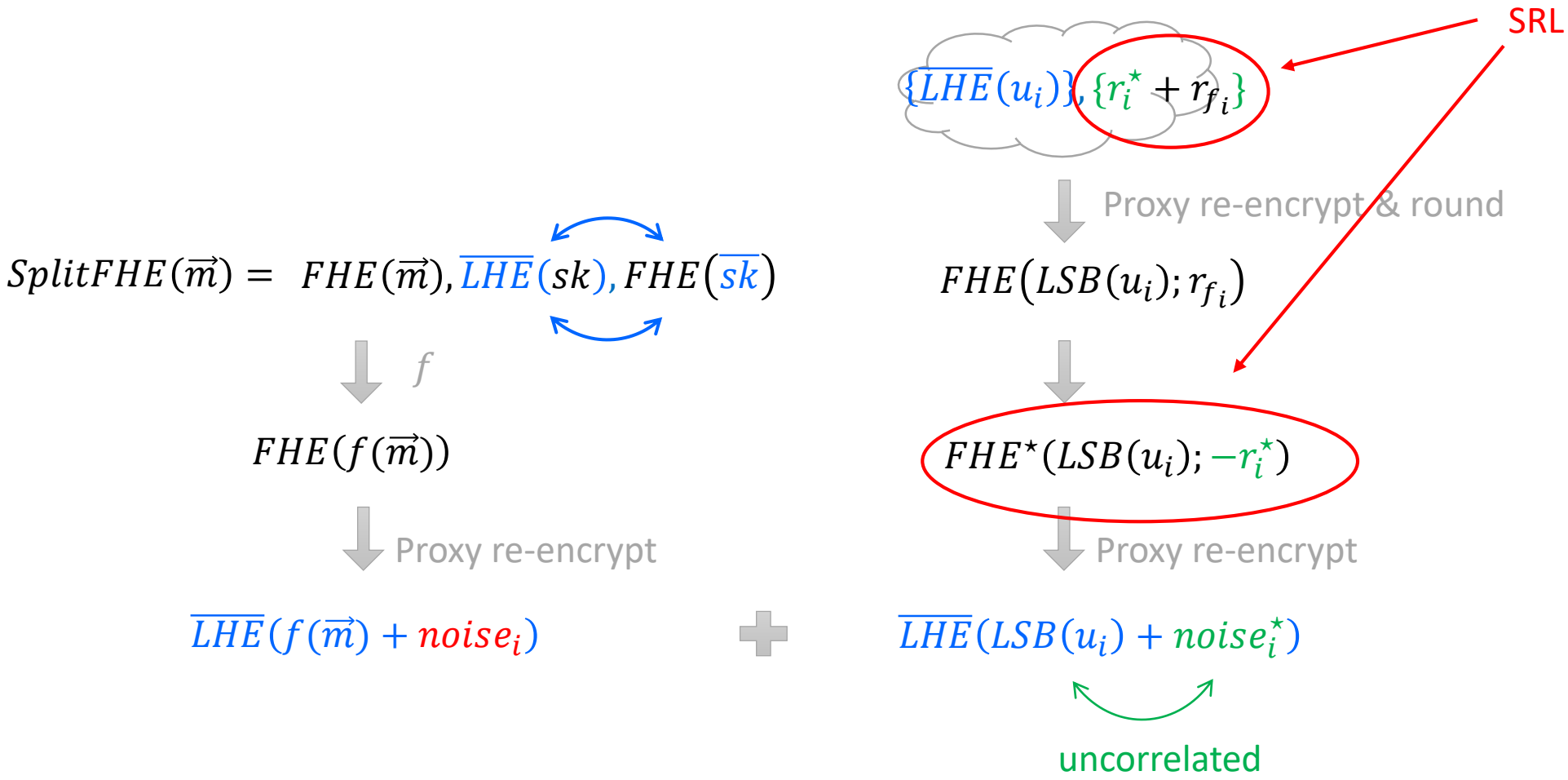
Circuit privacy of FHE: $(r_i^\star, r_{f_i} - r_i^\star) \approx_s (r_i^\star + r_{f_i}, -r_i^\star)$

Our Result



Circuit privacy of FHE: $(r_i^\star, r_{f_i} - r_i^\star) \approx_s (r_i^\star + r_{f_i}, -r_i^\star)$

Our Result



Circuit privacy of FHE: $(r_i^\star, r_{f_i} - r_i^\star) \approx_s (r_i^\star + r_{f_i}, -r_i^\star)$

Conclusion

iO from:

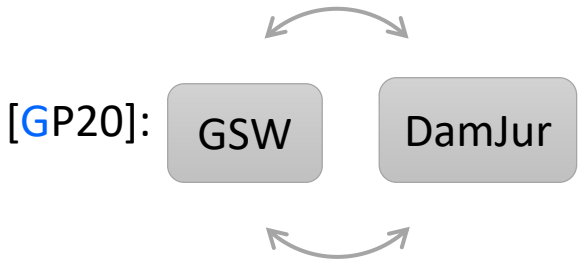
- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

Conclusion

iO from:

- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

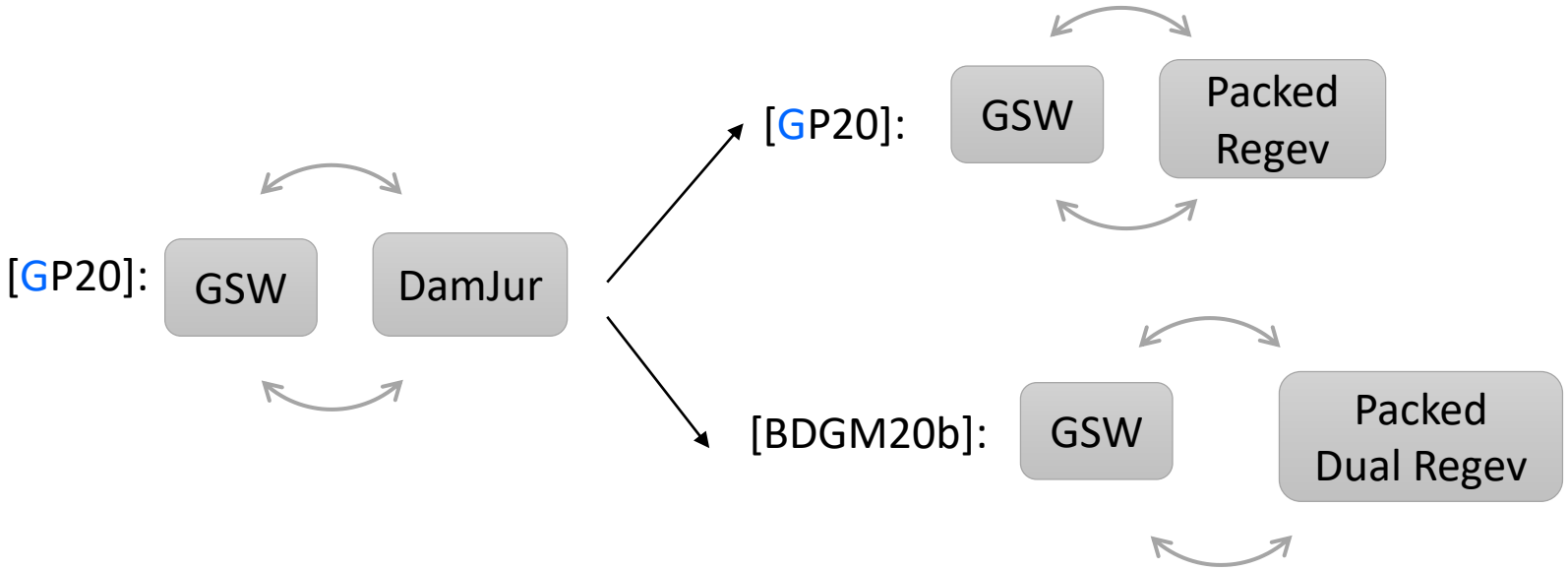
Related works:



Conclusion

iO from:
- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

Related works:

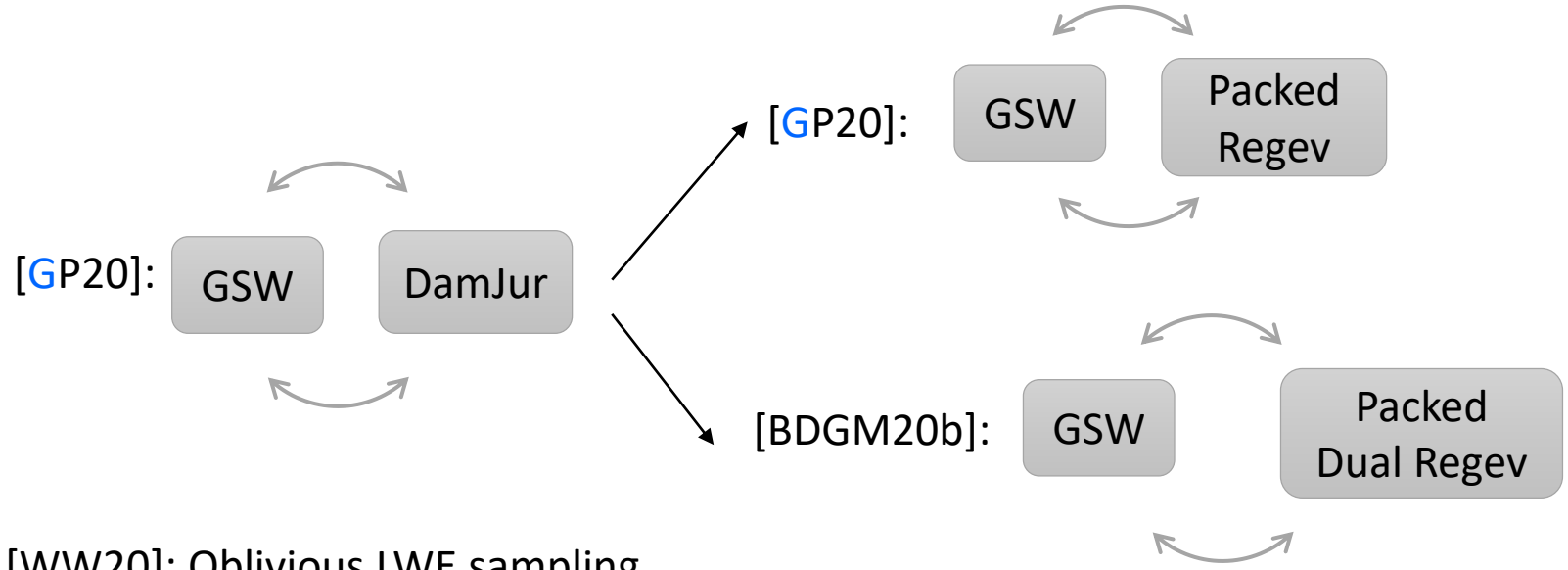


Conclusion

iO from:
- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

Related works:

Build upon [BDGM20a]



[WW20]: Oblivious LWE sampling

Conclusion

iO from:

- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

⟹ SRL circular security is qualitatively stronger than “plain” circular security

Conclusion

iO from:
- LWE with subexp. modulus-to-noise ratio
- strong CIRC conjecture w.r.t. SRL security and (GSW,P-Regev)

SRL circular security is qualitatively stronger than “plain” circular security

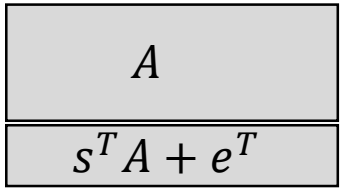
- **Provably** secure w/o key cycle
- **Natural** security notion

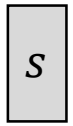
backed by a general design principle

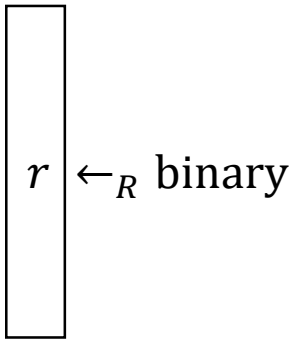
Extra Slides

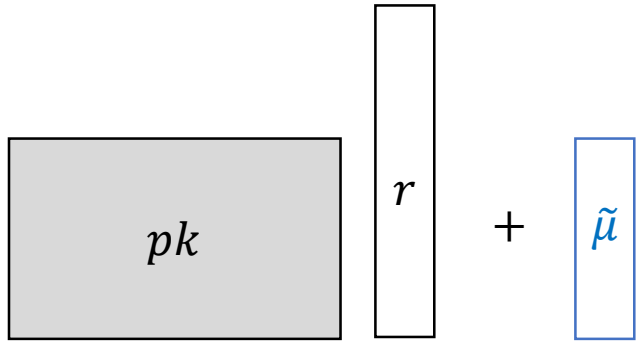
Packed-Regev LHE

Packed-Regev LHE

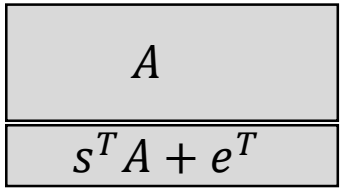
$pk =$ 

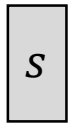
$sk =$ 

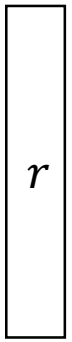
$Enc_{pk}(\mu \in \{0,1\})$: 

$ct =$ 

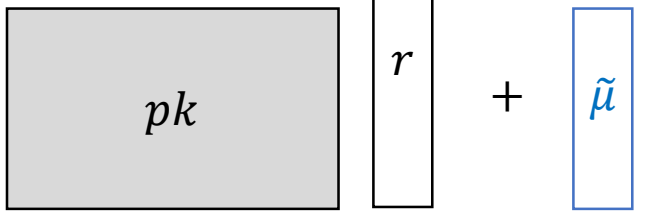
Packed-Regev LHE

$pk =$ 

$sk =$ 

$Enc_{pk}(\mu_1, \mu_2, \ldots \in \{0,1\})$: 

$\leftarrow_R$ binary

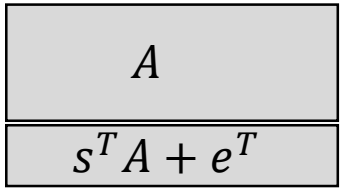
$ct =$ 

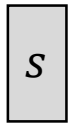
$+$

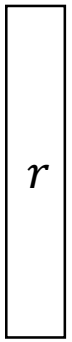
Proof:

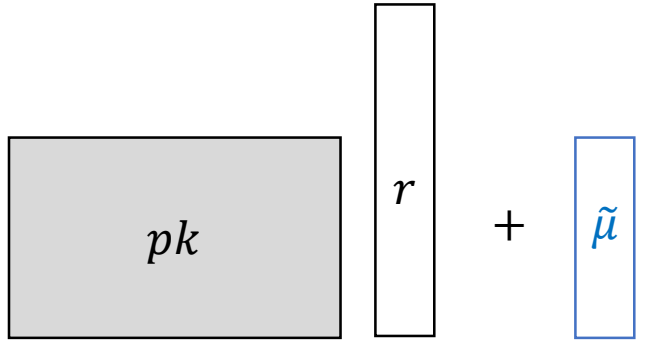
1) $pk \rightarrow$ uniform via LWE
2) Entropy of r masks μ

Packed-Regev LHE

$pk =$ 

$sk =$ 

$Enc_{pk}(\mu = \mu_1, \mu_2, \ldots \in \{0,1\})$: 

$ct =$ 

Proof:

1) $pk \rightarrow$ uniform via LWE
2) Entropy of r masks $\mu \Rightarrow |r| \geq |\mu|$ large randomness

Packed-Regev LHE

$pk =$ A_1 / $s^T A_1 + e_1^T$; A_2 / $s^T A_2 + e_2^T$; …

$sk =$ s

$Enc_{pk}(\mu_1, \mu_2, \ldots \in \{0,1\})$: $r \leftarrow_R$ binary

$ct =$ pk_1 / pk_2 / … $\cdot\, r +$ $\tilde{\mu}_1$ / $\tilde{\mu}_2$

Re-use r

Packed-Regev LHE

$pk =$ A_1 / $s^T A_1 + e_1^T$; A_2 / $s^T A_2 + e_2^T$; …

$sk =$ s

$Enc_{pk}(\mu_1, \mu_2, \ldots \in \{0,1\})$: $r \leftarrow_R$ binary

$ct =$ pk_1 / pk_2 / … $\cdot\, r +$ $\tilde{\mu}_1$ / $\tilde{\mu}_2$

Re-use r  Gaussian elimination → r

Packed-Regev LHE

$pk =$ A_1 / $s^T A_1 + e_1^T$; A_2 / $s^T A_2 + e_2^T$; …

$sk =$ s

$Enc_{pk}(\mu_1, \mu_2, \ldots \in \{0,1\})$: $r \leftarrow_R$ binary

$ct =$ pk_1 / pk_2 / … $\cdot\, r +$ $\tilde{\mu}_1 + \epsilon_1$; $+ \tilde{\mu}_2 + \epsilon_2$

Extra noises

Re-use r

Gaussian elimination → r

SRL Security Proof for GSW

SRL security of GSW

Real

Lossy

1

$pk \approx_{LWE} pk_{lossy}$

2

$Enc_{pk}(m) \xrightarrow[sk]{} m$

$Enc_{pk_{lossy}}(m) \approx_s Enc_{pk_{lossy}}(0)$

3

$Enc_{pk}(f(\vec{m})) \xrightarrow[sk]{} f(\vec{m})$

$ct_f = Enc_{pk_{lossy}}(f(\vec{m}); r_f)$

$\forall m_t \downarrow td$

r s.t. $ct_f = Enc_{pk_{lossy}}(m_t; r)$

SRL security of GSW

Real

Lossy

1 $pk = \begin{array}{|c|}\hline A \\ \hline s^T A + e^T \\ \hline \end{array} \approx_{LWE} pk_{lossy} = \begin{array}{|c|}\hline A \\ \hline u^T \\ \hline \end{array}$

2 $Enc_{pk}(m) = pk \cdot R + m$

$Enc_{pk_{lossy}}(m) = pk_{lossy} \cdot R + m \approx_{LOHL} uniform$

3 $ct_f = pk \cdot r_f + f(\vec{m})$

$ct_f = pk_{lossy} \cdot r_f + f(\vec{m})$

$\forall t$

$td \Rightarrow$ small r s.t. $pk_{lossy} \cdot r = t$

SRL security of GSW

Real

Lossy

1

$$pk = \begin{array}{|c|}\hline A \\ \hline s^T A + e^T \\ \hline \end{array} \approx_{LWE} pk_{lossy} = \begin{array}{|c|}\hline A \\ \hline u^T \\ \hline \end{array}$$

2

$$Enc_{pk}(m) = pk \cdot R + m$$

$$Enc_{pk_{lossy}}(m) = pk_{lossy} \cdot R + m \approx_{LOHL} uniform$$

3

$$ct_f = pk \cdot r_f + f(\vec{m})$$

$$ct_f = pk_{lossy} \cdot r_f + f(\vec{m})$$

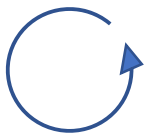
$\forall t$

td ⇒ small $\tilde{r}$ s.t. $pk_{lossy} \cdot \tilde{r} = t$

Lattice trapdoor [Ajt96,…]

SRL Security Proof

adversary



pk

$\vec{m}_0, \vec{m}_1$

$\overrightarrow{Enc}_{pk}(\vec{m}_b; \vec{r})$

$Enc_{pk}(0; r^\star)$

(f, α)

$r_f + r^\star$

b'

Real

$(pk, sk) \leftarrow Gen$

$r_f = Eval(f, \vec{r}, \vec{m}_b)$

SRL Security Proof

adversary

pk_{lossy}

$\vec{m}_0, \vec{m}_1$

$\overrightarrow{Enc}_{pk_{lossy}}(\vec{m}_b; \vec{r})$

$Enc_{pk_{lossy}}(0; r^\star)$

(f, α)

$r_f + r^\star$

b'

1 Switch to lossy

$(pk_{lossy}, td) \leftarrow Gen$

$r_f = Eval(f, \vec{r}, \vec{m}_b)$

SRL Security Proof

adversary

pk_{lossy}

$\vec{m}_0, \vec{m}_1$

$\overrightarrow{Enc}_{pk_{lossy}}(\vec{m}_b; \vec{r})$

$Enc_{pk_{lossy}}(0; r^\star)$

f, α

$\widetilde{r}_f + r^\star$

b'

3 Simulate $\widetilde{r}_f$ with td

$(pk_{lossy}, td) \leftarrow Gen$

$ct_f = \underbrace{pk_{lossy} \cdot r_f}_{t_f} + f(\overrightarrow{m_b})$

td ⇒ small $\widetilde{r}_f$ s.t. $pk_{lossy} \cdot r_f = t_f$

SRL Security Proof

adversary

pk_{lossy}

$\vec{m}_0, \vec{m}_1$

$\overrightarrow{Enc}_{pk_{lossy}}(\vec{0}; \vec{r})$

$Enc_{pk_{lossy}}(0; r^\star)$

f, α

$\tilde{r}_f + r^\star$

b'

2 Statistically hide $\vec{m}_b$

$(pk_{lossy}, td) \leftarrow Gen$

$ct_f = \underbrace{pk_{lossy} \cdot r_f}_{t_f} + f(\vec{m_b})$

td ⇒ small $\tilde{r}_f$ s.t. $pk_{lossy} \cdot r_f = t_f$