Communication complexity of the forge-and-lose technique

(@ secure evaluation of AES-128 and SHA-256 circuits)

Luís Brandão+

University of Lisbon / LaSIGE (Portugal) and Carnegie Mellon University (USA)

Crypto 2013 Rump Session

(Santa Barbara, USA, August 20)

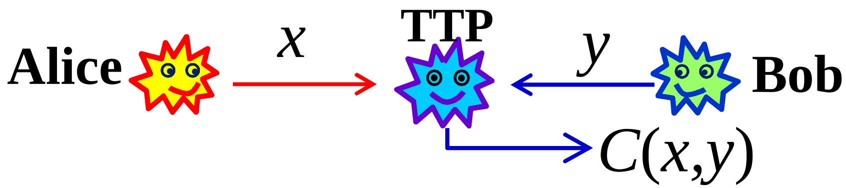
+ Ph.D. student, supported by the Portuguese Foundation for Science and Technology (FCT) through the Carnegie Mellon Portugal Program under Grant SFRH/BD/33770/2009.

S2PC via cut-and-choose of garbled circuits

© 2012-2013 Luís Brandão

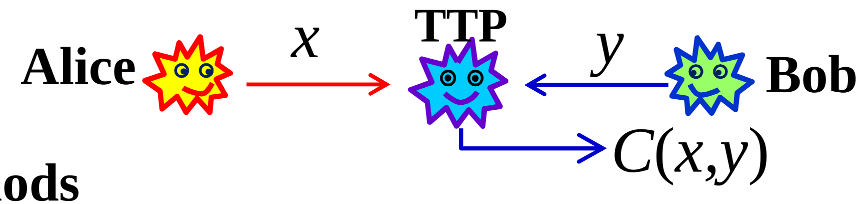
S2PC via cut-and-choose of garbled circuits

S2PC (ideal):

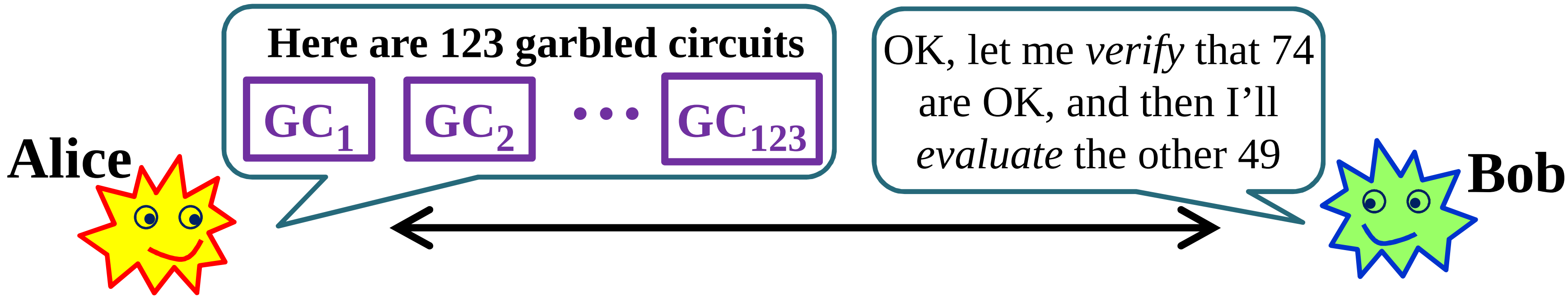


S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



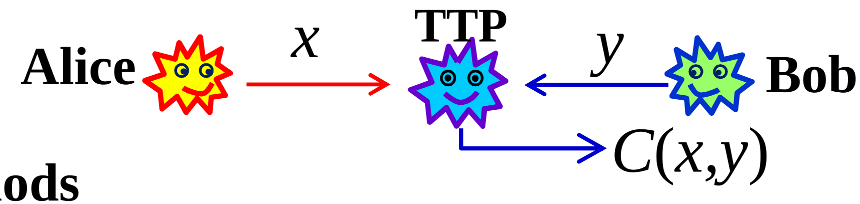
Usual C&C methods



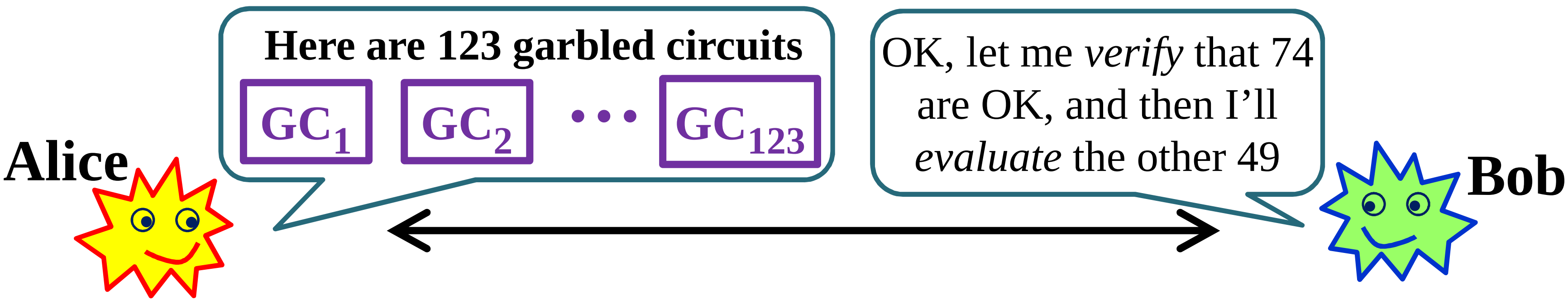
© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



Usual C&C methods

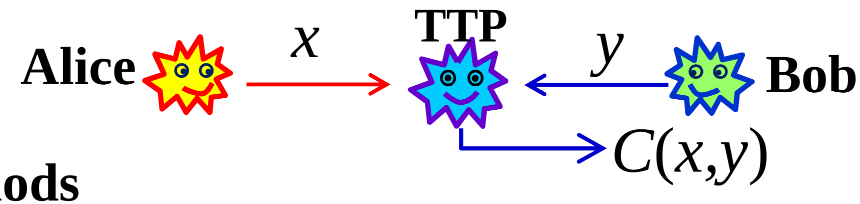


The output is OK **only if** **majority** of *evaluation* GCs is correct

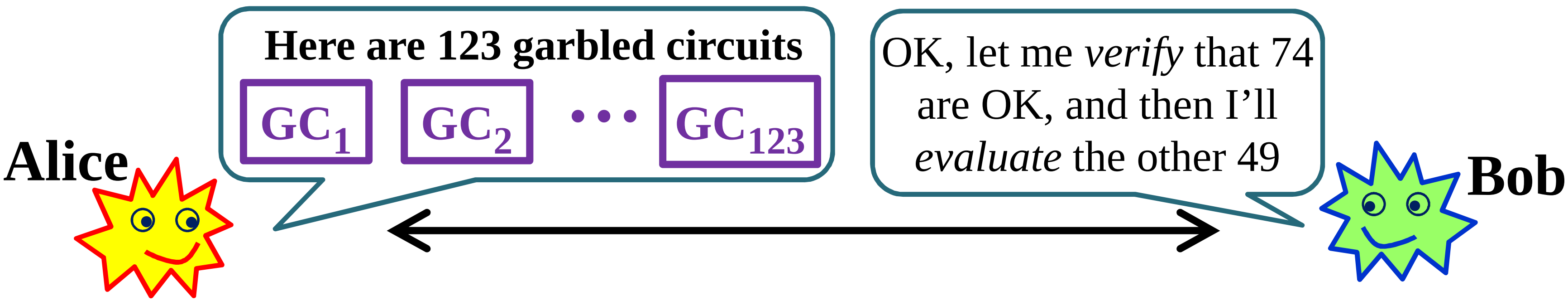
© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



Usual C&C methods



$$\Pr_{\text{error}} \approx 1.26 \cdot 2^{-0.32\,s}$$

The output is OK **only if** **majority** of *evaluation* GCs is correct

© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):

Alice $\xrightarrow{x}$ TTP $\xleftarrow{y}$ Bob

TTP $\rightarrow C(x,y)$

Usual C&C methods

Alice: **Here are 123 garbled circuits**

$\boxed{GC_1}$ $\boxed{GC_2}$ $\cdots$ $\boxed{GC_{123}}$

Bob: OK, let me *verify* that 74 are OK, and then I'll *evaluate* the other 49

$$\Pr_{\text{error}} \approx 1.26 \cdot 2^{-0.32\,\boxed{s}}$$

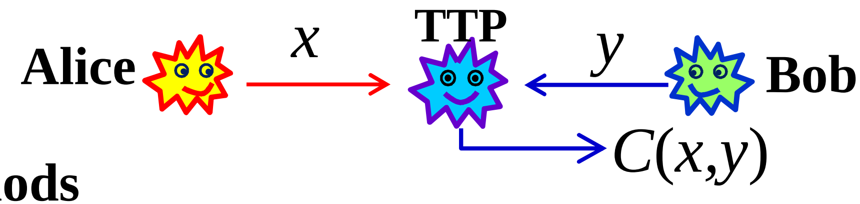
$s \equiv$ # GCs

The output is OK **only if majority** of *evaluation* GCs is correct

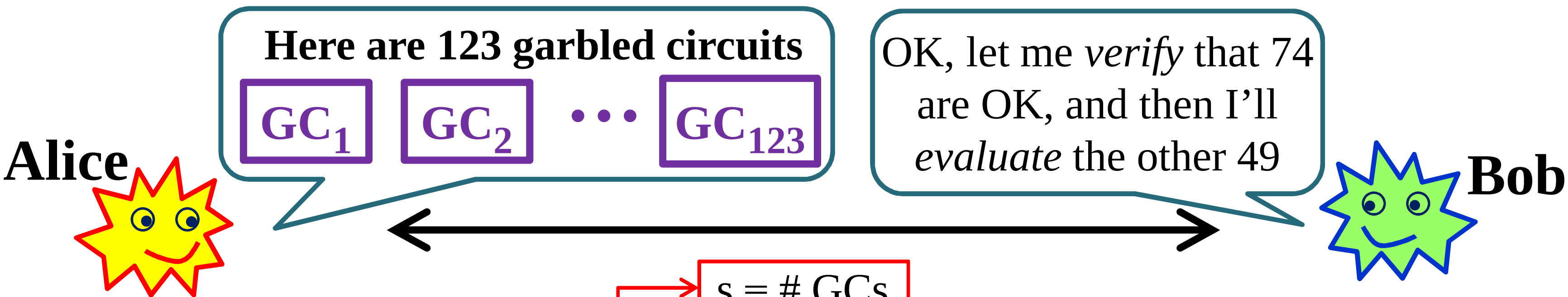
© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



Usual C&C methods



s ≡ # GCs

$$\mathrm{Pr}_{\mathrm{error}} \approx 1.26 \cdot 2^{-0.32\,\boxed{s}}$$

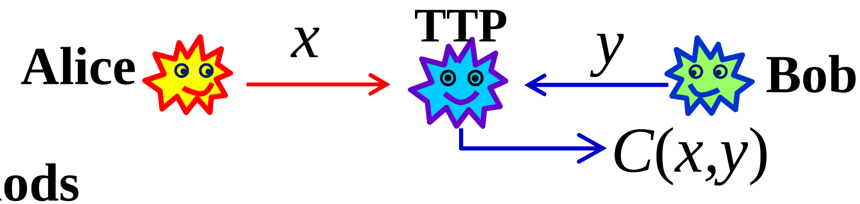
Example: **123** GCs for $\mathrm{Pr}_{\mathrm{error}} < \mathbf{2^{-40}}$

The output is OK **only if** **majority** of *evaluation* GCs is correct

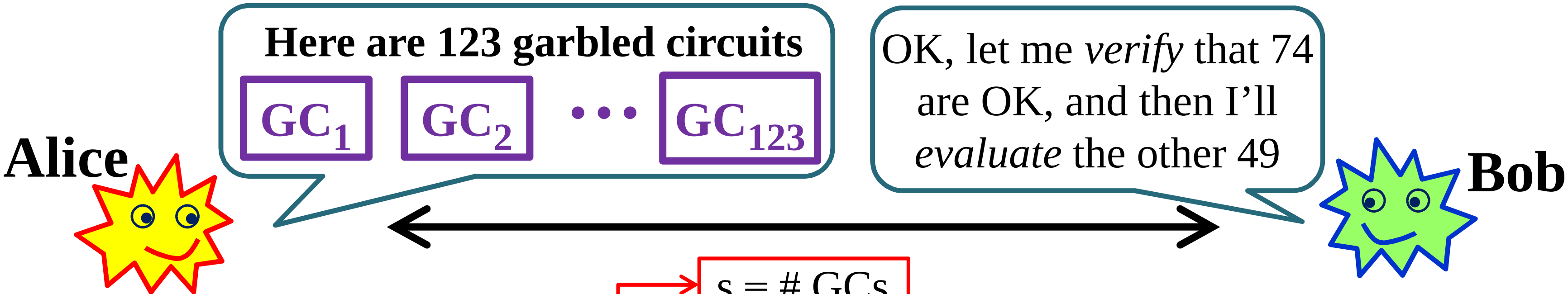
© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



Usual C&C methods



$$Pr_{error} \approx 1.26 \cdot 2^{-0.32\,\boxed{s}}$$

Example: **123** GCs for $Pr_{error} < 2^{-40}$

The output is OK **only if majority** of *evaluation* GCs is correct

---

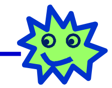
New optimal(?) C&C methods in 2013

The output is OK **if at least one** *evaluation* GC is correct

© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):

Alice  $\xrightarrow{x}$ TTP  $\xleftarrow{y}$  Bob

$\to C(x,y)$

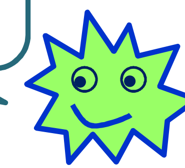
Usual C&C methods

Alice 

Here are 123 garbled circuits

GC_1 GC_2 ••• GC_{123}

OK, let me *verify* that 74 are OK, and then I'll *evaluate* the other 49

 Bob

$s \equiv \#$ GCs

$$\Pr_{error} \approx 1.26 \cdot 2^{-0.32\boxed{s}}$$

Example: **123** GCs for $\Pr_{error} < \mathbf{2^{-40}}$

The output is OK **only if majority** of *evaluation* GCs is correct

---

New optimal(?) C&C methods in 2013

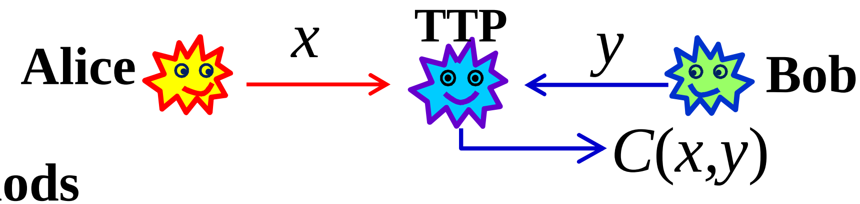
C&C proportions (*verify* vs. *evaluate*)	$\mathbf{Pr_{error}}$	**# GCs: $\mathbf{Pr_{error} \le 2^{-40}}$**
Fixed	$\approx 1.25 \cdot 2^{-s + (\log_2 s)/2}$	44
Variable	2^{-s}	40

The output is OK **if at least one** *evaluation* GC is correct

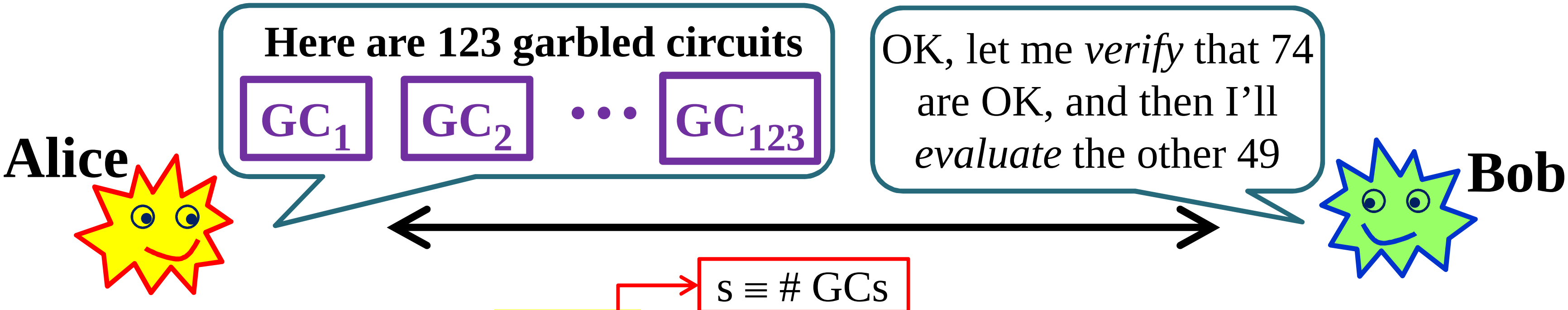
© 2012-2013 Luís Brandão

S2PC via cut-and-choose of garbled circuits

S2PC (ideal):



Usual C&C methods



$$\Pr_{error} \approx 1.26 \cdot 2^{-0.32\,s}$$

Example: **123** GCs for $\Pr_{error} < 2^{-40}$

The output is OK **only if majority** of *evaluation* GCs is correct

---

New optimal(?) C&C methods in 2013

C&C proportions (*verify* vs. *evaluate*)	$\mathbf{Pr_{error}}$	**# GCs: $\mathbf{Pr_{error} \leq 2^{-40}}$**
Fixed	$\approx 1.25 \cdot 2^{-s + (\log_2 s)/2}$	44
Variable	2^{-s}	40

The output is OK **if at least one** *evaluation* GC is correct

Compare against 123

© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)

© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)

© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session

© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

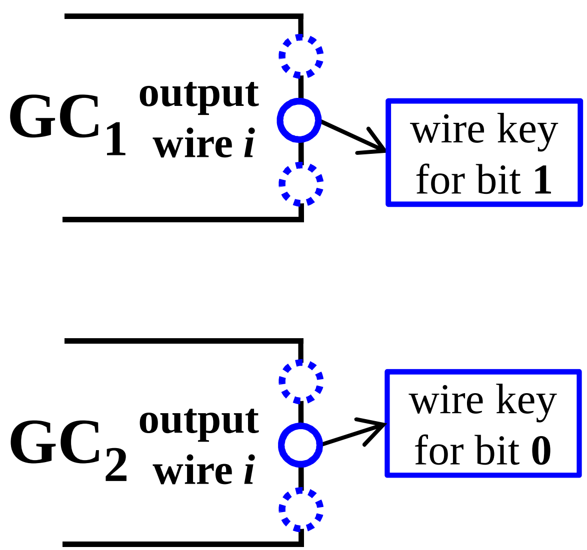
- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

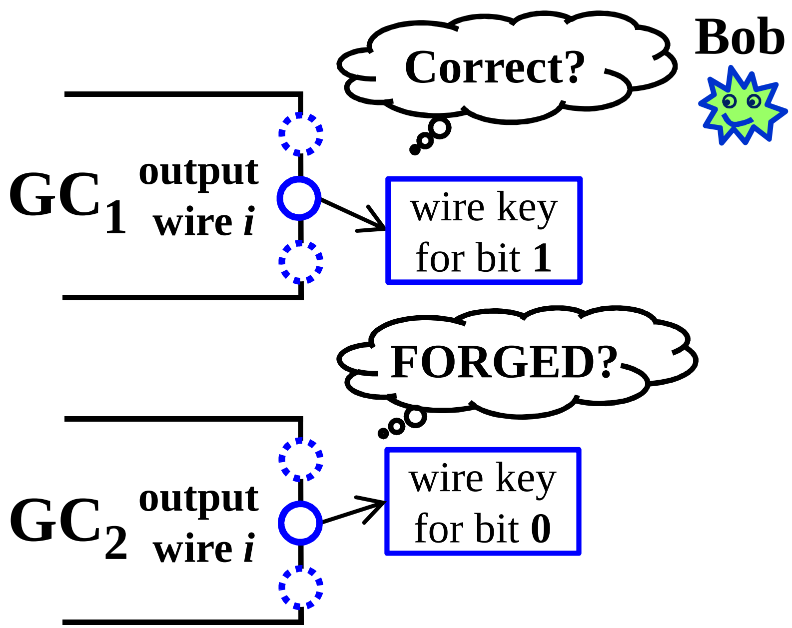
Forge-and-lose technique



Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

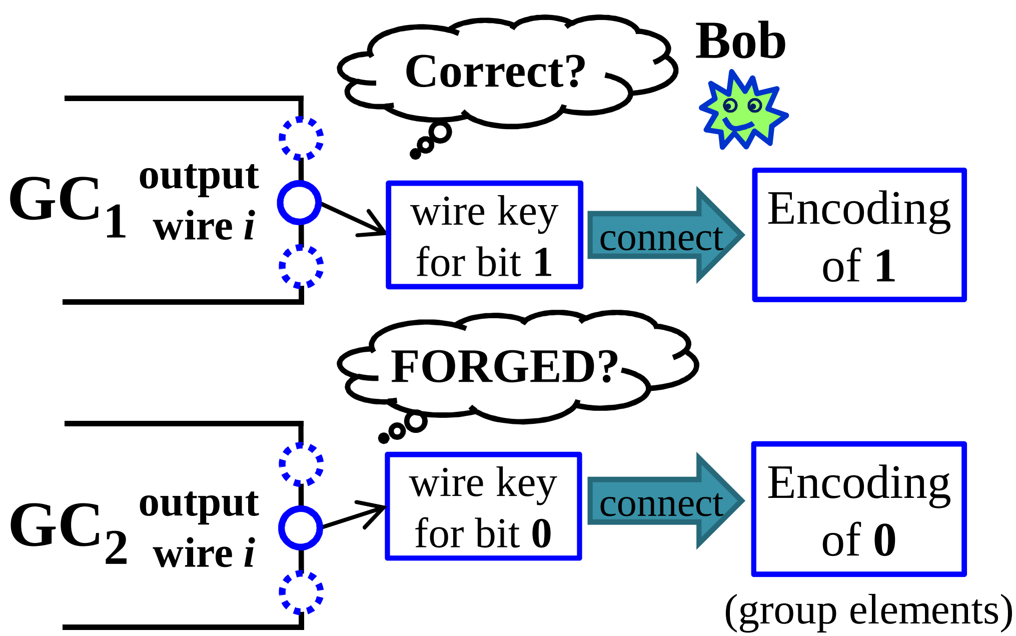
Forge-and-lose technique



Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

Forge-and-lose technique

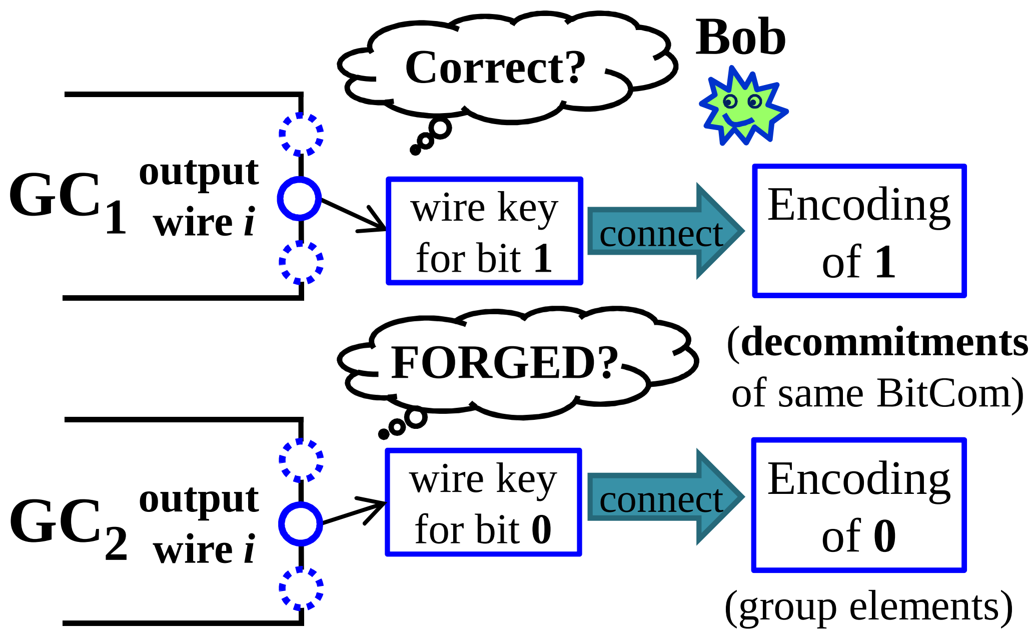


© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

Forge-and-lose technique

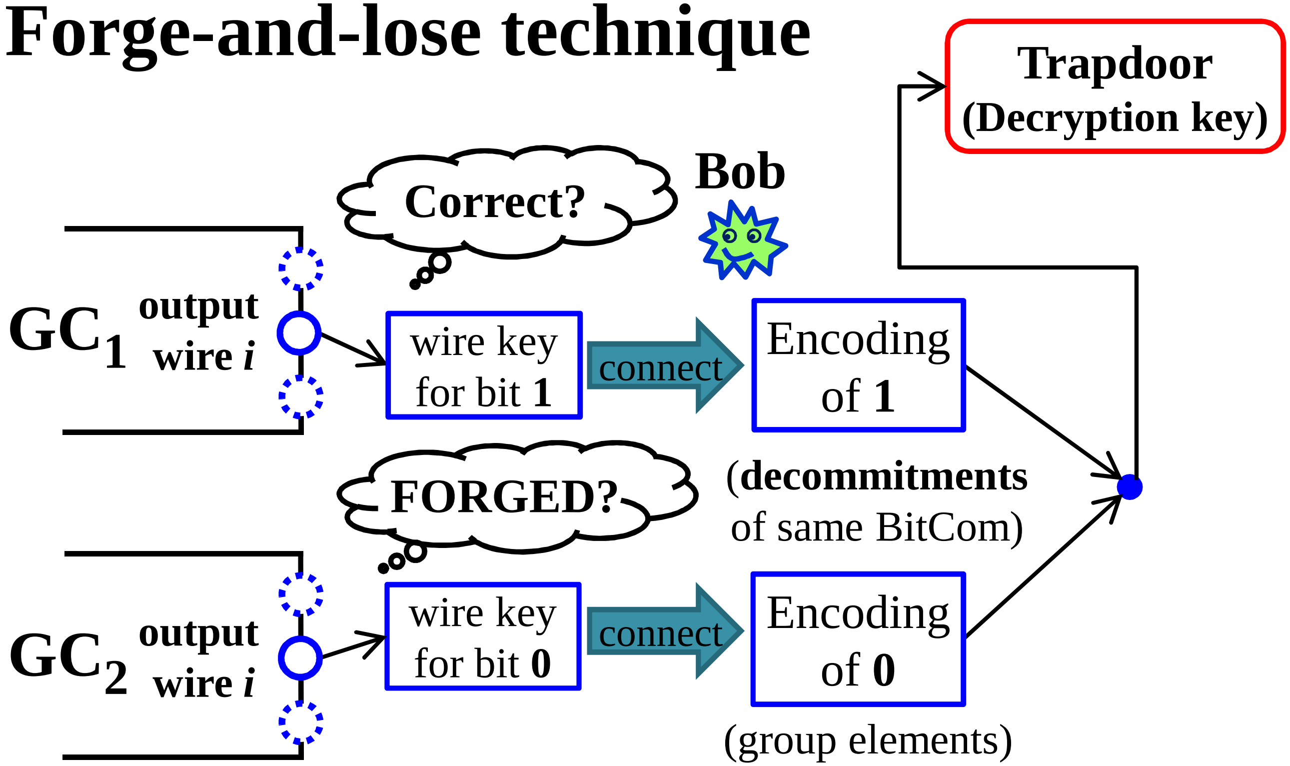


© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

Forge-and-lose technique

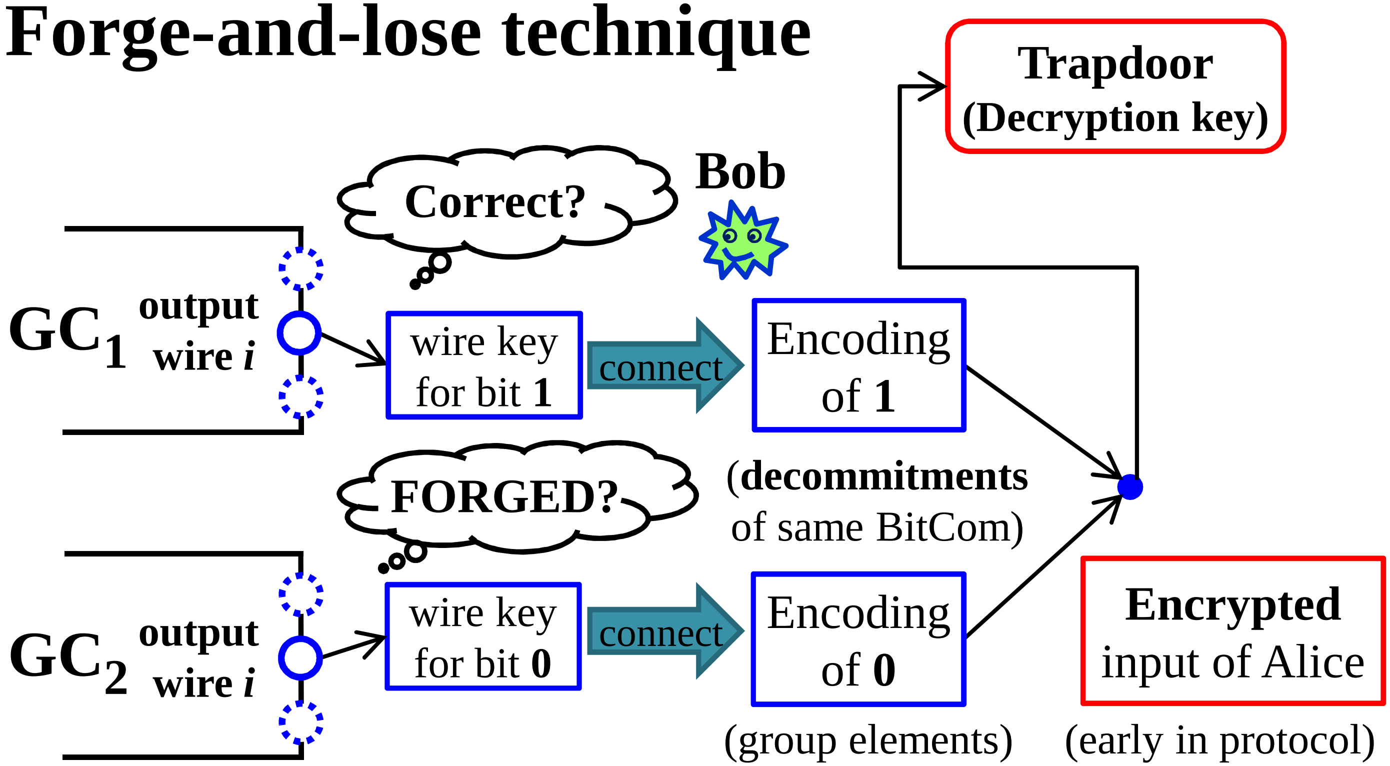


© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

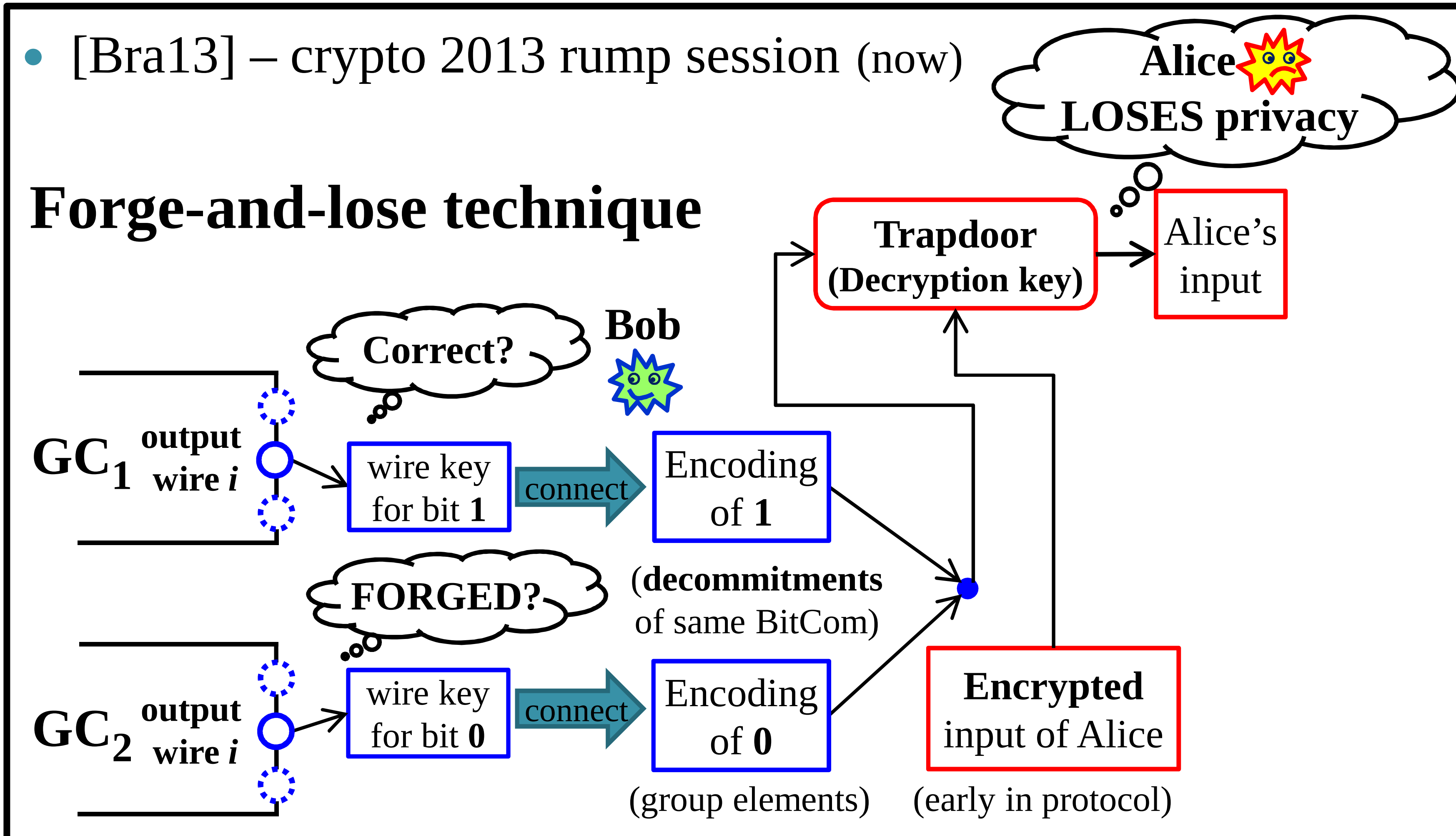
Forge-and-lose technique



© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

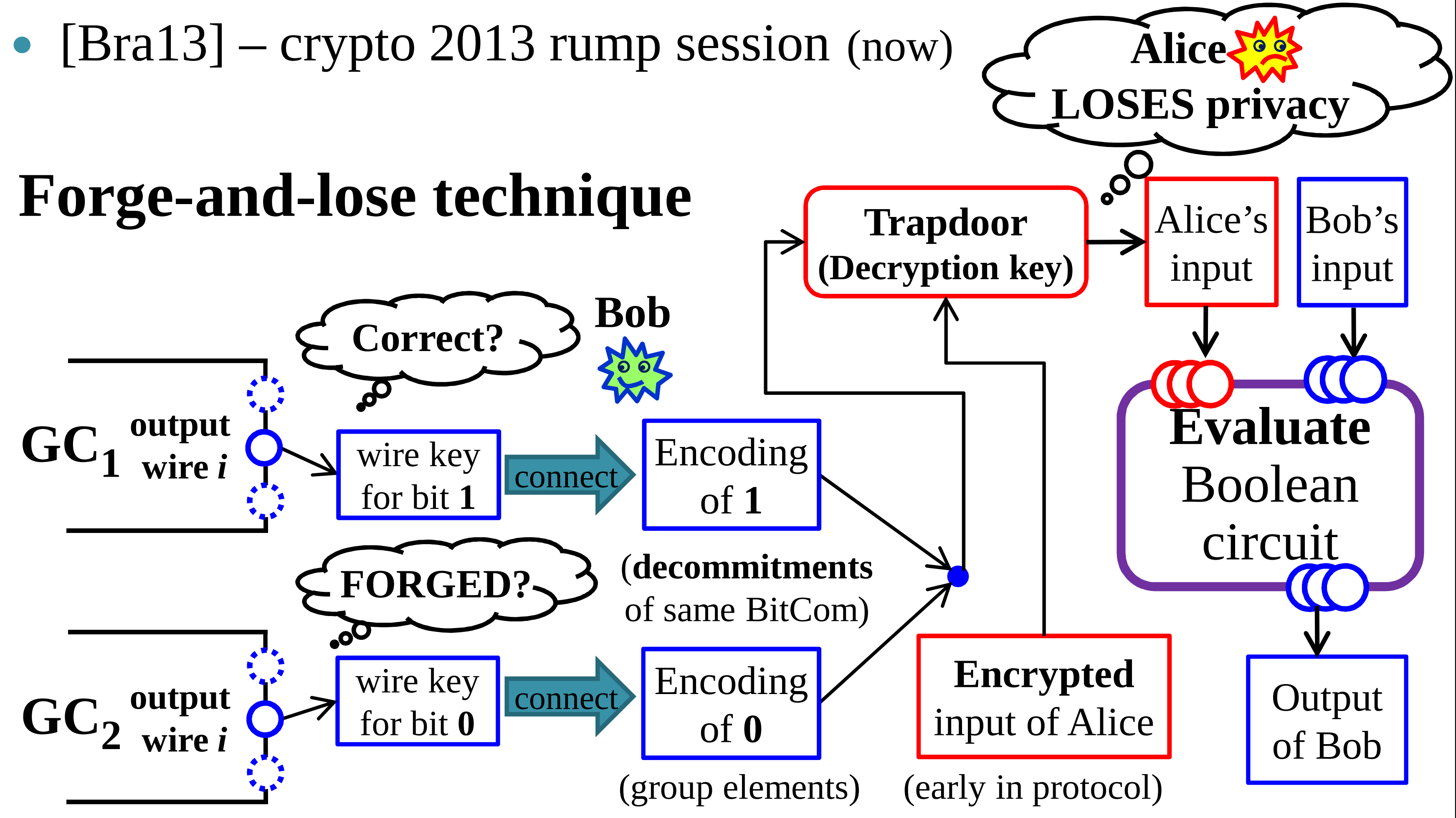
- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)



© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

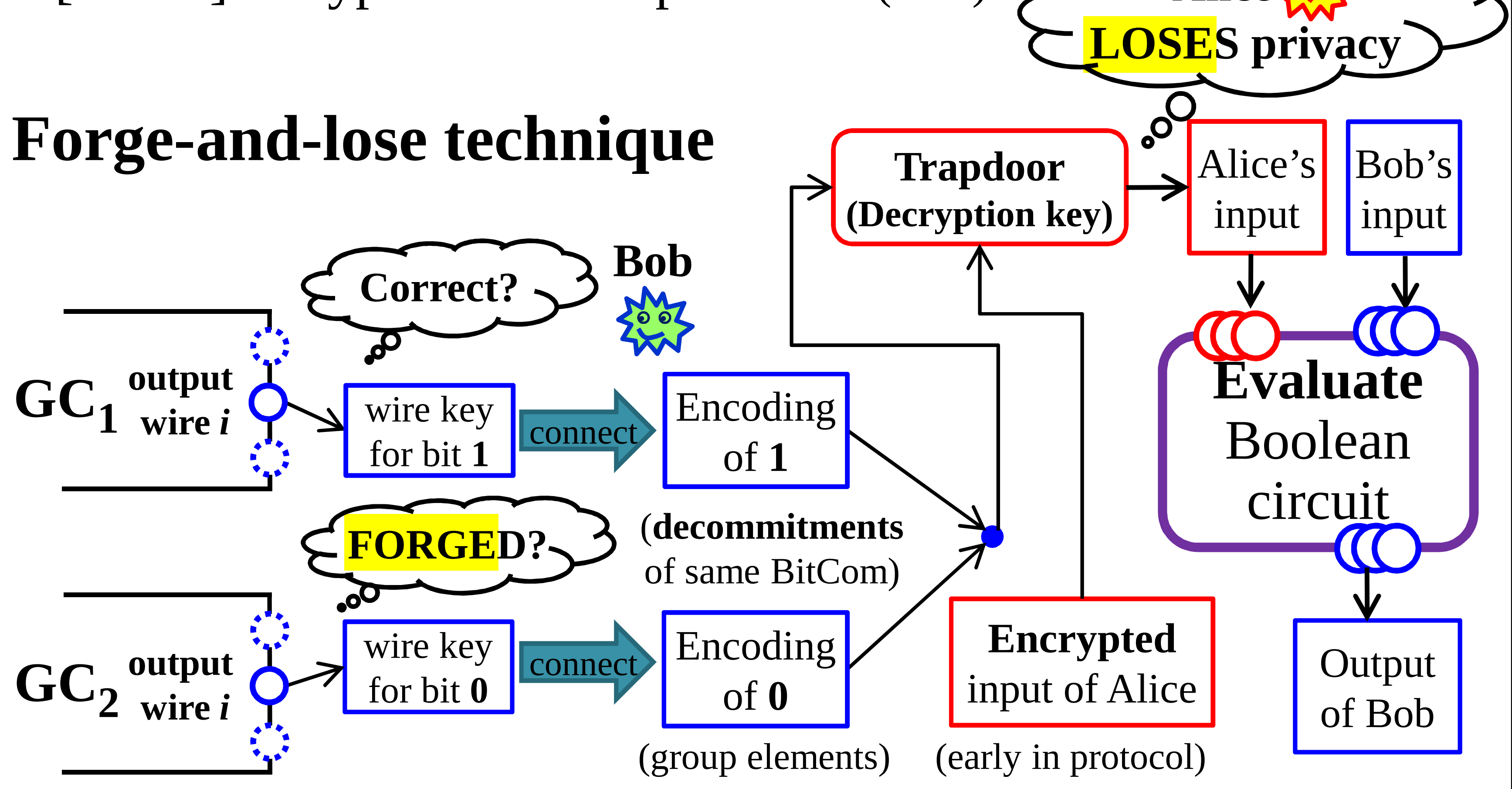
- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)



Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)

Forge-and-lose technique

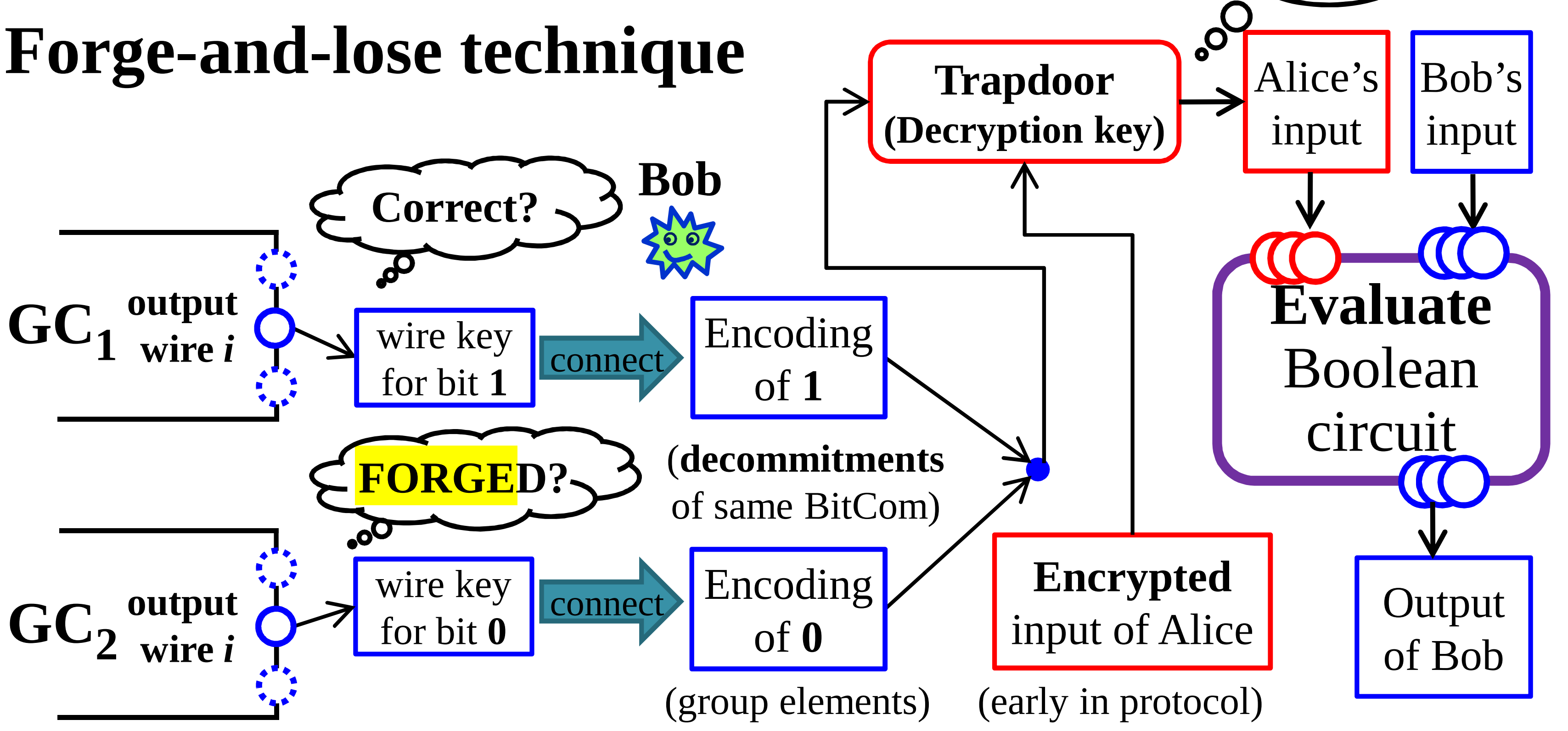


© 2012-2013 Luís Brandão

Three new optimal(?) C&C methods

- [Lin13] – crypto 2013 (Wednesday)
- [HKE13] – crypto 2013 (Wednesday)
- [Bra13] – crypto 2013 rump session (now)
  (and Asiacrypt 2013)

Forge-and-lose technique



© 2012-2013 Luís Brandão

Benchmarking communication in F&L

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits $\rightarrow$ 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128	
$\lvert C_\wedge \rvert$ [Bri13]	6,800	
$l_A = l_B = l'_B$	128	
$(l_A + l_B + l'_B)/\lvert C_\wedge \rvert$	5.6%	
s (# GCs)	41	123
Max # evaluation GCs	20	8
RSC@GCs	no	yes
GCs (Mb)	107	21
Total (Mb)	161	55
Overhead from non-GCs (%)	50%	163%

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128	
$\lvert C_\wedge \rvert$ [Bri13]	6,800	
$l_A = l_B = l'_B$	128	
$(l_A + l_B + l'_B)/\lvert C_\wedge \rvert$	5.6%	
s (# GCs)	41	123
Max # evaluation GCs	20	8
RSC@GCs	no	yes
GCs (Mb)	107	21
Total (Mb)	161	55
Overhead from non-GCs (%)	50%	163%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128	
$\lvert C_{\wedge} \rvert$ [Bri13]	6,800	
$l_A = l_B = l'_B$	128	
$(l_A + l_B + l'_B)/\lvert C_{\wedge} \rvert$	5.6%	
s (# GCs)	41	123
Max # evaluation GCs	20	8
RSC@GCs	no	yes
GCs (Mb)	107	21
Total (Mb)	161	55
Overhead from non-GCs (%)	50%	163%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128	
$\lvert C_{\wedge} \rvert$ [Bri13]	6,800	
$l_A = l_B = l'_B$	128	
$(l_A + l_B + l'_B)/\lvert C_{\wedge} \rvert$	5.6%	
s (# GCs)	41	123
Max # evaluation GCs	20	8
RSC@GCs	no	yes
GCs (Mb)	107	21
Total (Mb)	161	55
Overhead from non-GCs (%)	50%	163%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128	
$\lvert C_\wedge \rvert$ [Bri13]	6,800	
$l_A=l_B=l'_B$	128	
$(l_A+l_B+l'_B)/\lvert C_\wedge \rvert$	5.6%	
s (# GCs)	41	123
Max # evaluation GCs	20	8
RSC@GCs	no	yes
GCs (Mb)	107	21
Total (Mb)	161	55
Overhead from non-GCs (%)	50%	163%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128		SHA-256	
$\|C_\wedge\|$ [Bri13]	6,800		$\boxed{90,825}$	
$l_A=l_B=l'_B$	128		$\boxed{256}$	
$(l_A+l_B+l'_B)/\|C_\wedge\|$	5.6%		$\boxed{0.85\%}$	
s (# GCs)	41	123	41	123
Max # evaluation GCs	20	8	20	8
RSC@GCs	no	yes	no	yes
GCs (Mb)	107	21	1430	279
Total (Mb)	161	55	1545	345
Overhead from non-GCs (%)	50%	163%	8%	24%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128		SHA-256	
$\lvert C_\wedge \rvert$ [Bri13]	6,800		90,825	
$l_A = l_B = l'_B$	128		256	
$(l_A + l_B + l'_B)/\lvert C_\wedge \rvert$	5.6%		0.85%	
s (# GCs)	41	123	41	123
Max # evaluation GCs	20	8	20	8
RSC@GCs	no	yes	no	yes
GCs (Mb)	107	21	1430	279
Total (Mb)	161	55	1545	345
Overhead from non-GCs (%)	50%	163%	8%	24%

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128		SHA-256	
$\lvert C_\wedge \rvert$ [Bri13]	6,800		90,825	
$l_A = l_B = l'_B$	128		256	
$(l_A + l_B + l'_B)/\lvert C_\wedge \rvert$	5.6%		0.85%	
s (# GCs)	41	123	41	123
Max # evaluation GCs	20	8	20	8
RSC@GCs	no	yes	no	yes
GCs (Mb)	107	21	1430	279
Total (Mb)	161	55	1545	345
Overhead from non-GCs (%)	50%	163%	8%	24%

Some aspects

- **Intractability**: Quadratic Residuosity
- **#(exps)**: O(l)
- **Oblivious Transfers**: 2-out-of-1 OT
- **Proof security**: Ideal/real simulation (with rewinding)
- **BitComs input+output:** XOR-homomorphic ⇒ Efficient linkage of S2PCs

© 2012-2013 Luís Brandão

Benchmarking communication in F&L

- Crypto security: 128 bits → 3,072-bit Blum integers [NIST-SP800-57]
- Statistical security: 40 bits ($Pr_{error} \leq 2^{-40}$)
- Garbled gates: 384 bits
- Symmetric commitments: 256 / 384 bits

	AES-128		SHA-256	
$\lvert C_\wedge \rvert$ [Bri13]	6,800		90,825	
$l_A = l_B = l'_B$	128		256	
$(l_A + l_B + l'_B)/\lvert C_\wedge \rvert$	5.6%		0.85%	
s (# GCs)	41	123	41	123
Max # evaluation GCs	20	8	20	8
RSC@GCs	no	yes	no	yes
GCs (Mb)	107	21	1430	279
Total (Mb)	161	55	1545	345
Overhead from non-GCs (%)	50%	163%	8%	24%

(Further optimizations on the way)

Some aspects

- **Intractability**: Quadratic Residuosity
- **#(exps)**: O(l)
- **Oblivious Transfers**: 2-out-of-1 OT
- **Proof security**: Ideal/real simulation (with rewinding)
- **BitComs input+output:** XOR-homomorphic ⇒ Efficient linkage of S2PCs

© 2012-2013 Luís Brandão

Thanks

cut-and-chose

with

forge-and-lose!

lbrandao @ {fc.ul.pt, cmu.edu}

© 2012-2013 Luís Brandão