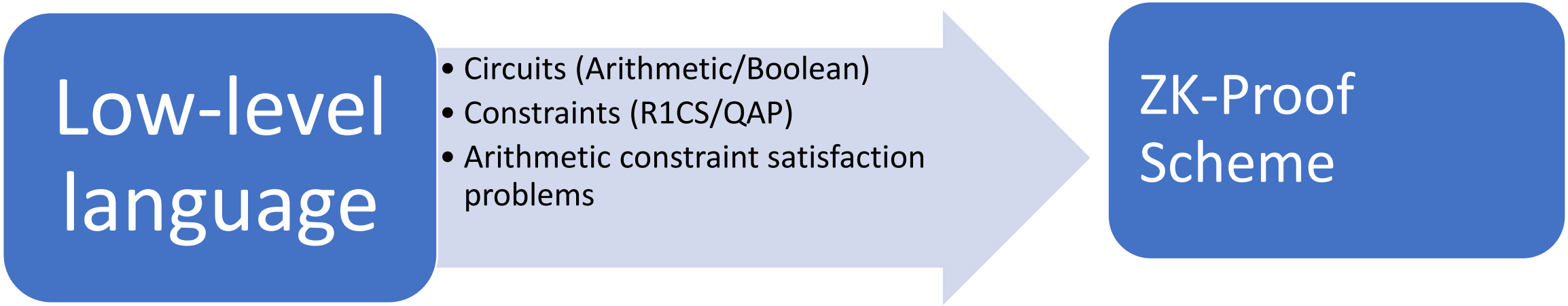
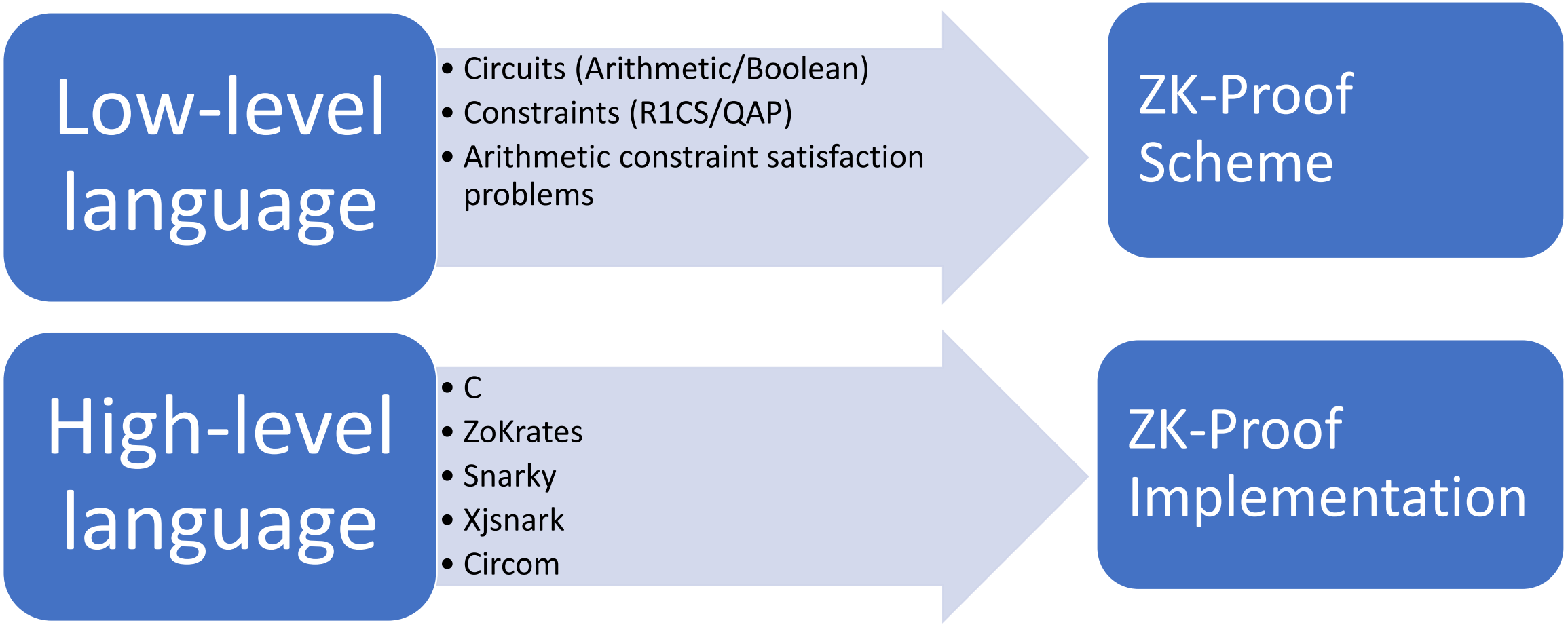
Interoperability of Zero-Knowledge Systems

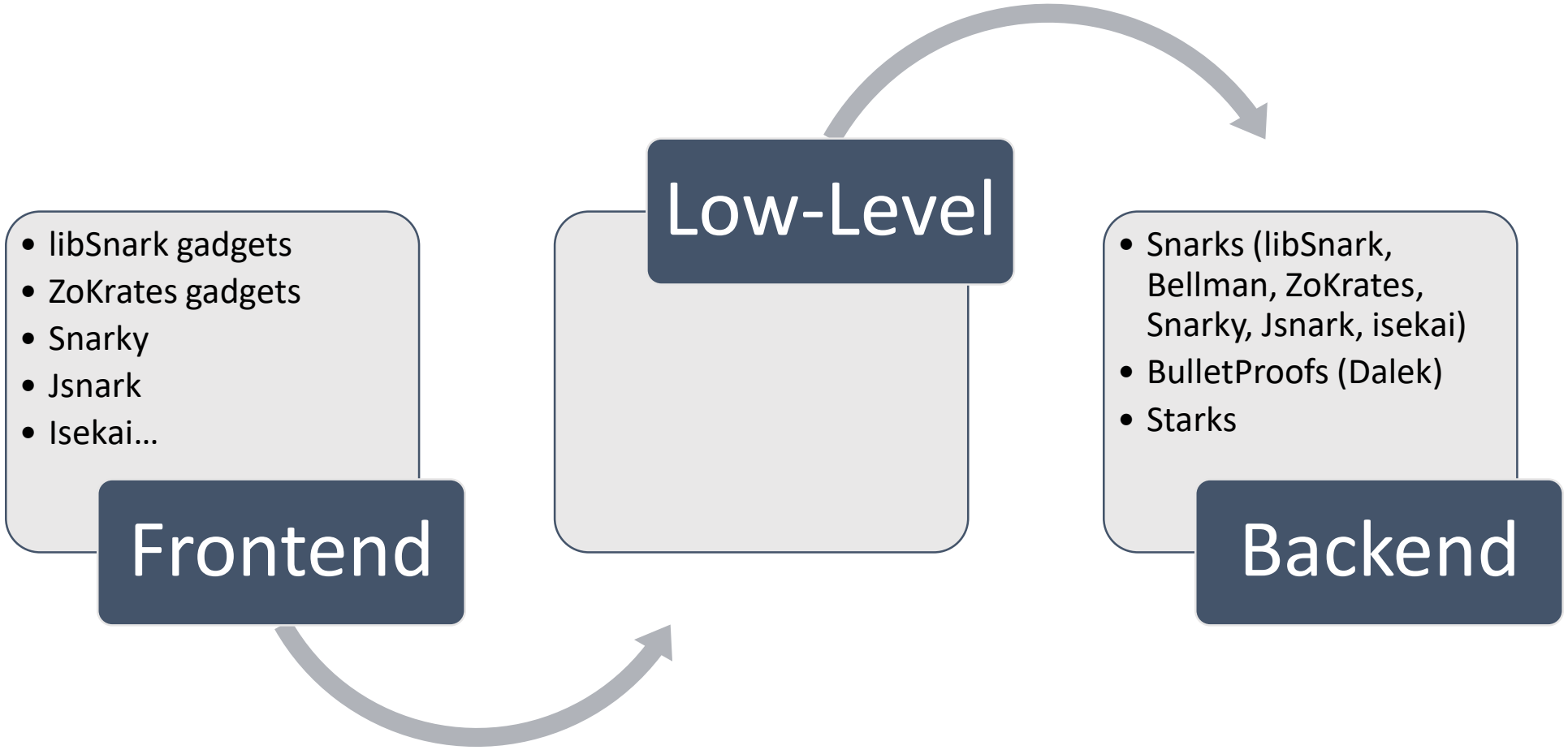
APRIL 2019

INTRODUCTION

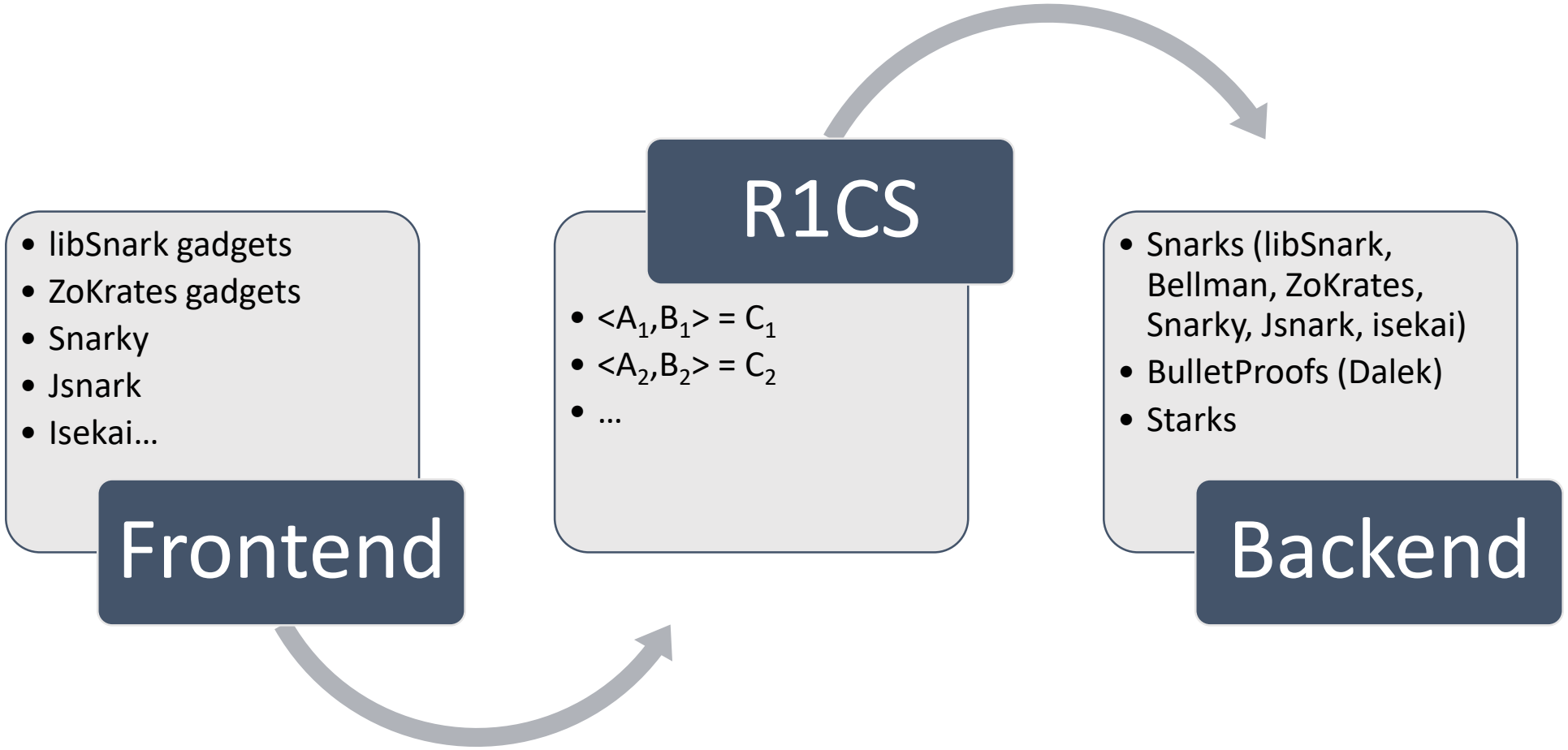


INTRODUCTION





ZK PROOF APPLICATION



INTEROPERABILITY WITH R1CS

R1CS

Set of bilinear equations $\langle A,B \rangle = C$

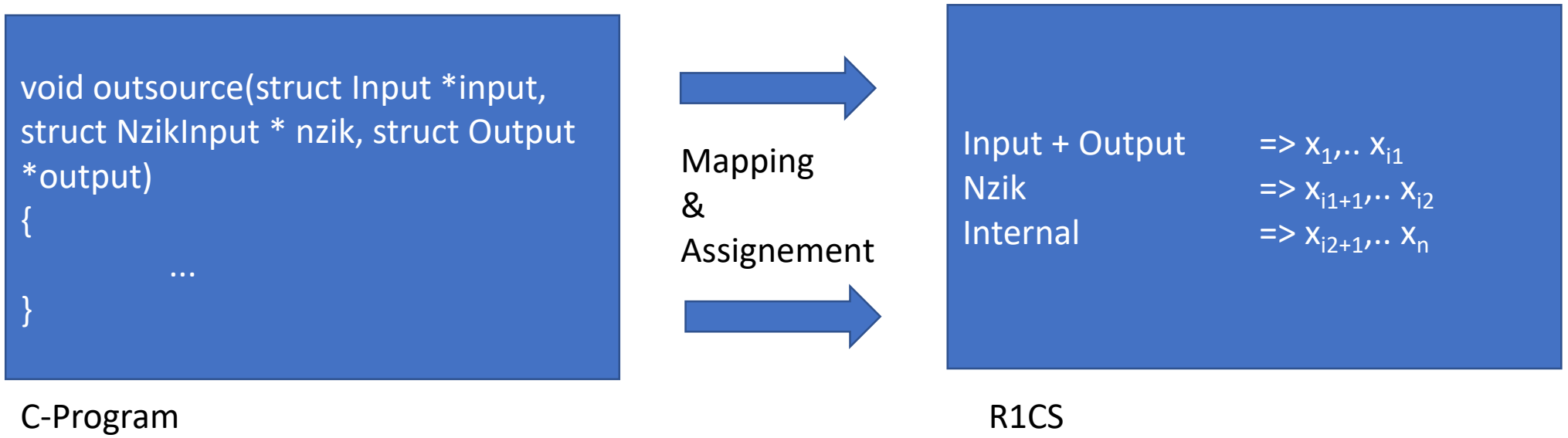
$(a_0 + a_1 * x_1 + \ldots + a_n * x_n) * (b_0 + b_1 * x_1 + \ldots + b_n * x_n) = c_0 + c_1 * x_1 + \ldots + c_n * x_n$

a_i , b_i , c_i are coefficients in a finite field

x_i are the variables of the system

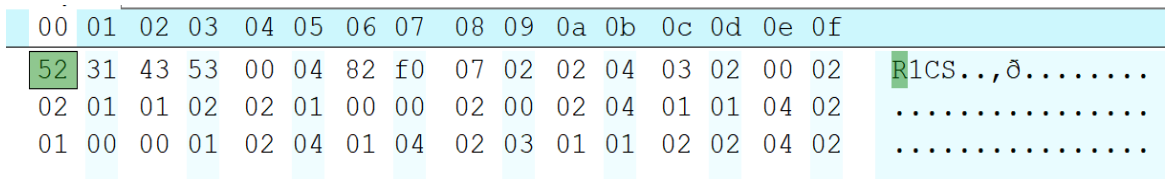
R1CS REDUCTION

- R1CS variables represent the input data (both public and zero-knowledge) of the high-level statements as well internal variables
- The mapping of the variables is done during the R1CS reduction



EXISTING FORMATS


```
{"variables":["ONE", "res", "A_0", "A_1",
"A_2", "B_0", "B_1", "B_2"],
"constraints":[[{"2":1},{"5":1},{"0":0,"8":1}],
[{"3":1},{"6":1},{"8":-1,"9":1}],
[{"4":1},{"7":1},{"9":-1,"1":1}]
]}
```

JSON

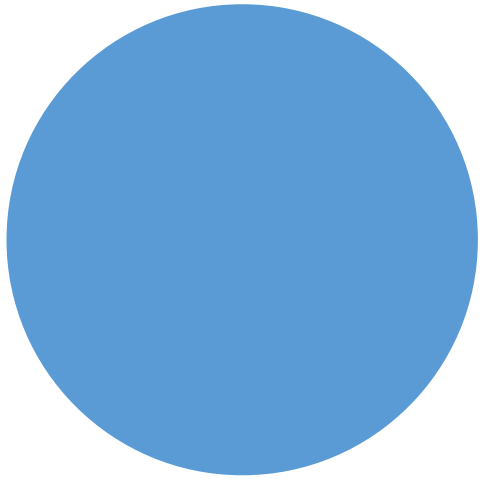
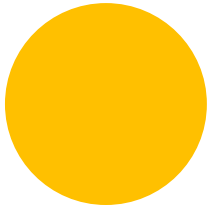
- https://github.com/barryWhiteHat/libsnark-tutorial/blob/master/zksnark_element/r1cs.json

BINARY (.R1CS)

- https://github.com/str4d/zk/tree/r1cs-file

BINARY (.ZKP2)

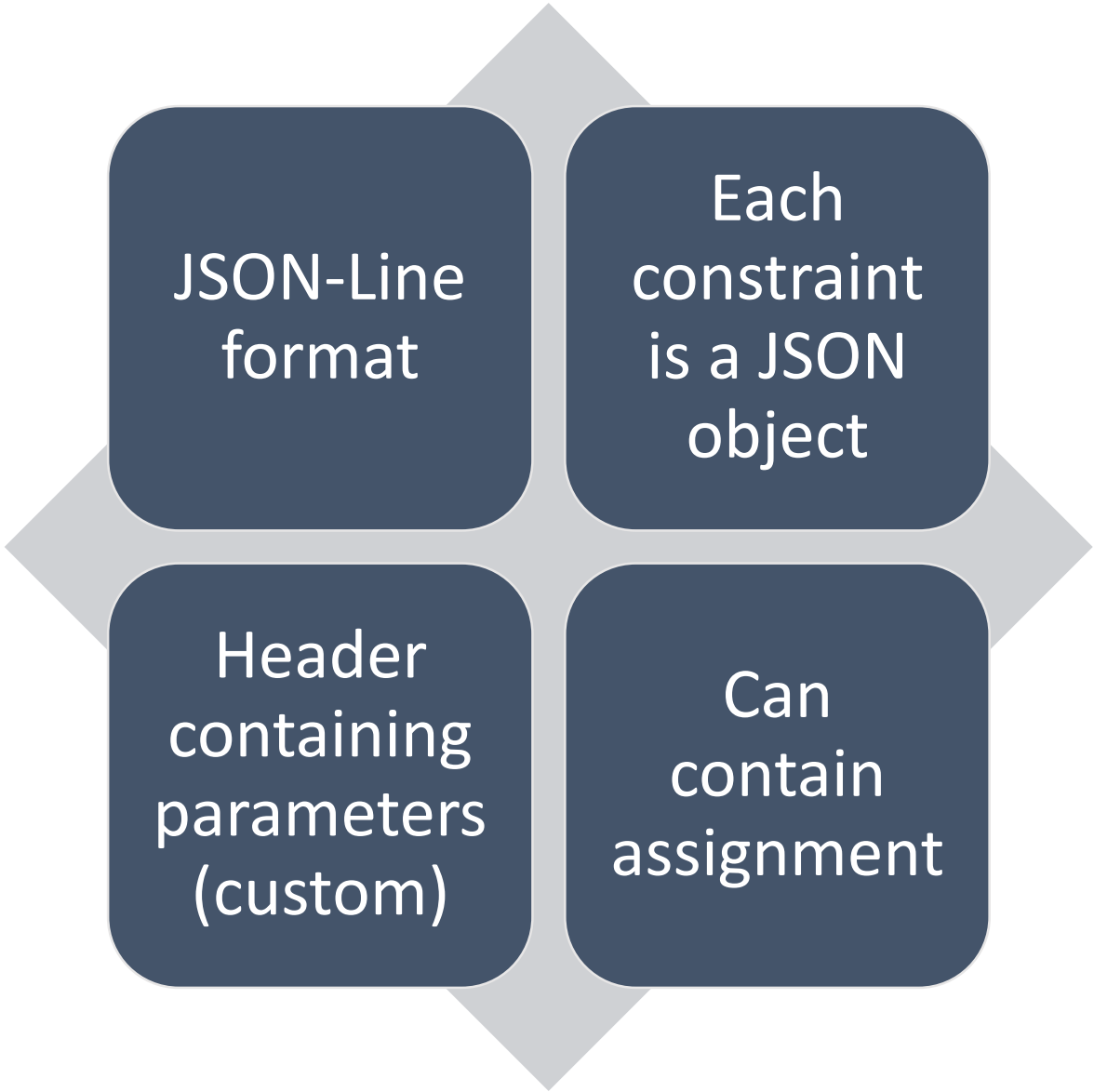
- https://github.com/QED-it/gadget_standard/

J-R1CS

A JSON-Lines format for R1CS

J-R1CS


JSON-Line format
Each constraint is a JSON object
Header containing parameters (custom)
Can contain assignment

HEADER


```
{
   "r1cs": {
            "version":"1.0",
            "field_characteristic":"13358119985180779799717823584852756340 1",
            "extension_degree":1,
            "instances":3,
            "witnesses":5,
            "constraints":2000,
            "optimized":true
    }
}
```

CONSTRAINTS

{"A":[[2464,"1"]],"B":[[2399,"1"],[2400,"1"]],"C":[[2530,"1"]]}
{"A":[[12,"1"],[2464,"218882428718392752222464057452572750885483644004160343436982041865758084956 16"]],"B":[[2397,"1"],[2398,"1"]],"C":[,[2531,"1"]]}
{"A":[[2464,"1"]],"B":[[11,"1"]],"C":[[2532,"1"]]}
{"A":[[12,"1"],[2464,"218882428718392752222464057452572750885483644004160343436982041865758084956 16"]],"B":[[2399,"1"],[2400,"1"]],"C":[[2533,"1"]]}
{"A":[[88,"1"]],"B":[[12,"0"]],"C":[[2534,"1"]]}
{"A":[[12,"1"],[88,"218882428718392752222464057452572750885483644004160343436982041865758084956 16"]],"B":[[12,"0"]],"C":[[2535,"1"]]}
{"A":[[352,"1"]],"B":[[12,"1"]],"C":[[2536,"1"]]}
{"A":[[12,"1"],[352,"218882428718392752222464057452572750885483644004160343436982041865758084956 16"]],"B":[[2534,"1"],[2535,"1"]],"C":[,[2537,"1"]]}
{"A":[[616,"1"]],"B":[[12,"2"]],"C":[[2538,"1"]]}
{"A":[[12,"1"],[616,"218882428718392752222464057452572750885483644004160343436982041865758084956 16"]],"B":[[2536,"1"],[2537,"1"]],"C":[[2539,"1"]]}

.....

ASSIGNMENTS (OPTIONAL)

{ “assignment":
{ "inputs":["0","1","0","1","3","8","5","4","2","1","9","1","8","1","0", "1","3","8","5","4","2","1","14757395258967641 2929","9"],
"witnesses": ["1","1","1","0","0","0","1","0","0","0","0","0","0","0", "0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","9","0","0","0","0","0","0","0","3","0","4","0","0","4","0", "4","0","4","0","4","9","0","0","1","24320269857599194691384895272508083431720404889351149270775782429528676106 24","0","1","0","1","27360303 589799094027808007181571593860685455500520042929622755233219760619 52",
"0","0","0","1","18761351033005093047639776353077664361612883771785172 29459846073135069299624 3","0","14757395258967641 2929","0"],
"names": [[-1,"IN_A"],[-2,"IN_B"],.... [1,"W_A"],[2,"W_B"],....]}
}

PRO

- **Extensibility**
- **Implementation**
- **Lightweight**
- **Interoperability**
- **Readability**
- **Scalability**

IMPLEMENTATION

- C++ sample implementation available in the call for standard proposal
- Isekai (https://github.com/sikoba/isekai) generates J-R1CS files from a C program (work*in*progress)

EXAMPLE

- Getting the median of 3 elements with isekai

```
#include "ex4.h"

void outsource(struct Input *input, struct NzikInput * nzik, struct Output *output)
{
		int tmp  = 0;
		if (nzik->a2 < nzik->a1)
		{
				tmp = nzik->a1;
				nzik->a1 = nzik->a2;
				nzik->a2 = tmp;
		}
		if (nzik->a3 < nzik->a2)
		{
				tmp = nzik->a3;
				nzik->a3 = nzik->a2;
				nzik->a2 = tmp;
		}
		if (nzik->a2 < nzik->a1)
		{
				tmp = nzik->a1;
				nzik->a1 = nzik->a2;
				nzik->a2 = tmp;
		}
		output->x = nzik->a2 ;
}
```

EXAMPLE (16KB)

{"r1cs":{"constraint_nb":111,"extension_degree":1,"field_characteristic":"21888242871839275222246405745257275088548364400416034343698204186575808495617","instance_nb":2,"version":"1.0","witness_nb":110}}
{"A":[[0,"0"],[6,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[6,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[7,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[7,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[8,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[8,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[9,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[9,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[10,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[10,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[11,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[11,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[12,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[12,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[13,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[13,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[14,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[14,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[15,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[15,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[16,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[16,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[17,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[17,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[18,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[18,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[19,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[19,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[20,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[20,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[21,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[21,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[22,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[22,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[23,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[23,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[24,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[24,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[25,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[25,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[26,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[26,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[27,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[27,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[28,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[28,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[29,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[29,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[30,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[30,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[31,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[31,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[32,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[32,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[33,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[33,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[34,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[34,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[35,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[35,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[36,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[36,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[37,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[37,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[38,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[38,"1"]],"C":[[0,"0"]]}

EXAMPLE

{"A":[[0,"0"],[3,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[4,"1"]],"B":[[0,"1"]],"C":[[0,"0"],[6,"1"],[7,"2"],[8,"4"],[9,"8"],[10,"16"],[11,"32"],[12,"64"],[13,"128"],[14,"256"],[15,"512"],[16,"1024"],[17,"2048"],[18,"4096"],[19,"8192"],[20,"16384"],[21,"32768"],[22,"65536"],[23,"131072"],[24,"262144"],[25,"524288"],[26,"1048576"],[27,"2097152"],[28,"4194304"],[29,"8388608"],[30,"16777216"],[31,"33554432"],[32,"67108864"],[33,"134217728"],[34,"268435456"],[35,"536870912"],[36,"1073741824"],[37,"2147483648"],[38,"4294967296"]]}
{"A":[[0,"0"],[37,"1"]],"B":[[0,"0"],[3,"1"]],"C":[[0,"0"],[39,"1"]]}
{"A":[[0,"0"],[1,"1"],[37,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"]],"B":[[0,"0"],[4,"1"]],"C":[[0,"0"],[40,"1"]]}
{"A":[[0,"0"],[41,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[41,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[42,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[42,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[43,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[43,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[44,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[44,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[45,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[45,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[46,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[46,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[47,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[47,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[48,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[48,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[49,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[49,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[50,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[50,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[51,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[51,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[52,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[52,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[53,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[53,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[54,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[54,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[55,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[55,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[56,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[56,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[57,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[57,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[58,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[58,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[59,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[59,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[60,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[60,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[61,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[61,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[62,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[62,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[63,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[63,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[64,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[64,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[65,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[65,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[66,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[66,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[67,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[67,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[68,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[68,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[69,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[69,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[70,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[70,"1"]],"C":[[0,"0"]]}

EXAMPLE

{"A":[[0,"0"],[71,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[71,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[72,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[72,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[73,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[73,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[5,"1"],[39,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[40,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"]],"B":[[0,"1"]],"C":[[0,"0"],[41,"1"],[42,"2"],[43,"4"],[44,"8"],[45,"16"],[46,"32"],[47,"64"],[48,"128"],[49,"256"],[50,"512"],[51,"1024"],[52,"2048"],[53,"4096"],[54,"8192"],[55,"16 384"],[56,"32768"],[57,"65536"],[58,"131072"],[59,"262144"],[60,"524288"],[61,"1048576"],[62,"2097152"],[63,"4194304"],[64,"8388608"],[65,"16777216"],[66,"33554432"],[67,"67108864"],[68,"1342 17728"],[69,"268435456"],[70,"536870912"],[71,"1073741824"],[72,"2147483648"],[73,"4294967296"]]}
{"A":[[0,"0"],[72,"1"]],"B":[[0,"0"],[5,"1"]],"C":[[0,"0"],[74,"1"]]}
{"A":[[0,"0"],[1,"1"],[72,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"]],"B":[[0,"0"],[39,"1"],[40,"1"]],"C":[[0,"0"],[75,"1"]]}
{"A":[[0,"0"],[37,"1"]],"B":[[0,"0"],[4,"1"]],"C":[[0,"0"],[76,"1"]]}
{"A":[[0,"0"],[1,"1"],[37,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"]],"B":[[0,"0"],[3,"1"]],"C":[[0,"0"],[77,"1"]]}
{"A":[[0,"0"],[78,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[78,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[79,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[79,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[80,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[80,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[81,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[81,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[82,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[82,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[83,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[83,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[84,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[84,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[85,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[85,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[86,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[86,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[87,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[87,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[88,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[88,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[89,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[89,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[90,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[90,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[91,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[91,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[92,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[92,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[93,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[93,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[94,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[94,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[95,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[95,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[96,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[96,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[97,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[97,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[98,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[98,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[99,"1"]],"B":[[0,"2188824287183927522224640574525727508854836440041603434369820418657580849561 6"],[99,"1"]],"C":[[0,"0"]]}

EXAMPLE

{"A":[[0,"0"],[100,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[100,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[101,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[101,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[102,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[102,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[103,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[103,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[104,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[104,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[105,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[105,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[106,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[106,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[107,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[107,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[108,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[108,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[109,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[109,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[110,"1"]],"B":[[0,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[110,"1"]],"C":[[0,"0"]]}
{"A":[[0,"0"],[74,"1"],[75,"1"],[76,"21888242871839275222246405745257275088548364400416034343698204186575808495616"],[77,"21888242871839275222246405745257275088548364400416034343698204186575808495616"]],"B":[[0,"1"]],"C":[[0,"0"],[78,"1"],[79,"2"],[80,"4"],[81,"8"],[82,"16"],[83,"32"],[84,"64"],[85,"128"],[86,"256"],[87,"512"],[88,"1024"],[89,"2048"],[90,"4096"],[91,"8192"],[92,"16384"],[93,"32768"],[94,"65536"],[95,"131072"],[96,"262144"],[97,"524288"],[98,"1048576"],[99,"2097152"],[100,"4194304"],[101,"8388608"],[102,"16777216"],[103,"33554432"],[104,"67108864"],[105,"134217728"],[106,"268435456"],[107,"536870912"],[108,"1073741824"],[109,"2147483648"],[110,"4294967296"]]}
{"A":[[0,"0"],[109,"1"]],"B":[[0,"0"],[76,"1"],[77,"1"]],"C":[[0,"0"],[111,"1"]]}
{"A":[[0,"0"],[1,"1"],[109,"21888242871839275222246405745257275088548364400416034343698204186575808495616"]],"B":[[0,"0"],[74,"1"],[75,"1"]],"C":[[0,"0"],[112,"1"]]}
{"A":[[0,"0"],[1,"1"]],"B":[[0,"0"],[111,"1"],[112,"1"]],"C":[[0,"0"],[2,"1"]]}

{"assignment":{"inputs":["1","8"],"witnesses":["4","13","8","1","0","0","1","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","13","0","0","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","1","0","1","1","1","1","8","0","0","4","0","0","1","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","8"]}}

EXAMPLE (ARITHMETIC CIRCUIT)

```
total 131
input 0 # one-input
nizkinput 1 # input
nizkinput 2 # input
nizkinput 3 # input
const-mul-0 in 1 <0> out 1 <4> # zero
const-mul-neg-1 in 1 <1> out 1 <5> # multiply-by-constant -1
add in 2 <2 5> out 1 <6> # CmpLT Isekai::DFGExpr - Isekai::DFGExpr
split in 1 <6> out 33 <7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39> # SplitBus
mul in 2 <38 1> out 1 <40> # cond trueterm
const-mul-neg-1 in 1 <38> out 1 <41> # cond minuscond
add in 2 <0 41> out 1 <42> # cond negcond
mul in 2 <42 2> out 1 <43> # cond falseterm
add in 2 <40 43> out 1 <44> # cond result
const-mul-neg-1 in 1 <44> out 1 <45> # multiply-by-constant -1
add in 2 <3 45> out 1 <46> # CmpLT Isekai::DFGExpr - Isekai::DFGExpr
split in 1 <46> out 33 <47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79> # SplitBus
mul in 2 <78 3> out 1 <80> # cond trueterm
const-mul-neg-1 in 1 <78> out 1 <81> # cond minuscond
add in 2 <0 81> out 1 <82> # cond negcond
mul in 2 <82 44> out 1 <83> # cond falseterm
add in 2 <80 83> out 1 <84> # cond result
mul in 2 <38 2> out 1 <85> # cond trueterm
const-mul-neg-1 in 1 <38> out 1 <86> # cond minuscond
add in 2 <0 86> out 1 <87> # cond negcond
mul in 2 <87 1> out 1 <88> # cond falseterm
add in 2 <85 88> out 1 <89> # cond result
const-mul-neg-1 in 1 <89> out 1 <90> # multiply-by-constant -1
add in 2 <84 90> out 1 <91> # CmpLT Isekai::DFGExpr - Isekai::DFGExpr
split in 1 <91> out 33 <92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124> # SplitBus
mul in 2 <123 89> out 1 <125> # cond trueterm
const-mul-neg-1 in 1 <123> out 1 <126> # cond minuscond
add in 2 <0 126> out 1 <127> # cond negcond
mul in 2 <127 84> out 1 <128> # cond falseterm
add in 2 <125 128> out 1 <129> # cond result
mul in 2 <0 129> out 1 <130> # output-cast
output 130 #
```

GUILLAUME DREVON
gd@sikoba.com