Malicious Garbled Circuits

CS 598 DH

Today's objectives

Review IT MACs

Construct maliciously secure garbling

Setting

Semi-honest Security "......Previously

Malicious Security

Zero Knowledge

General-Purpose Tools

GMW Protocol

Multi-party

Multi-round

Garbled Circuit

Constant Round

Two Party

Primitives

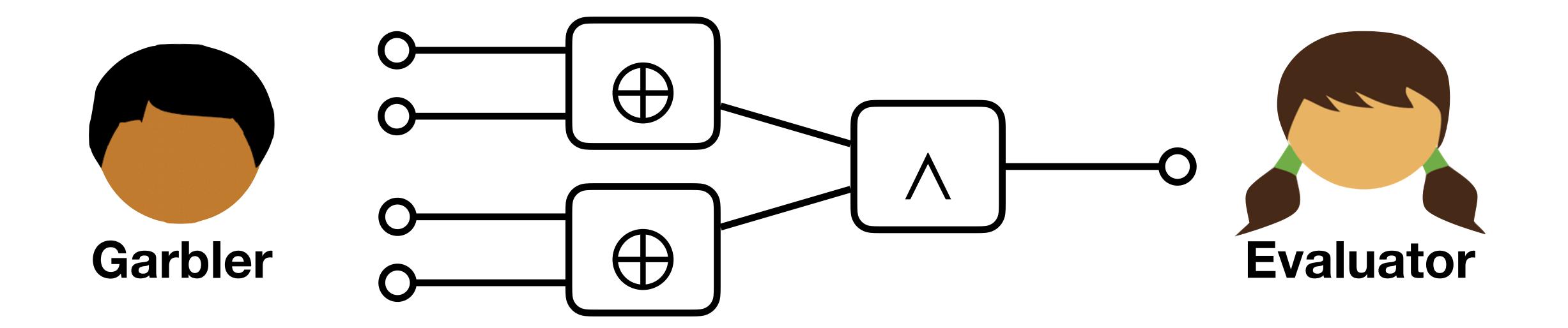
Oblivious Transfer

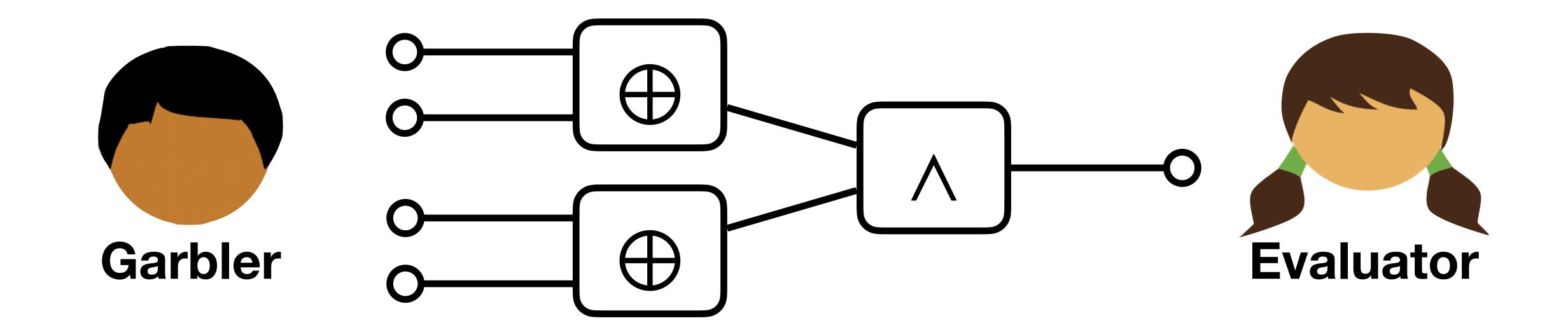
Today

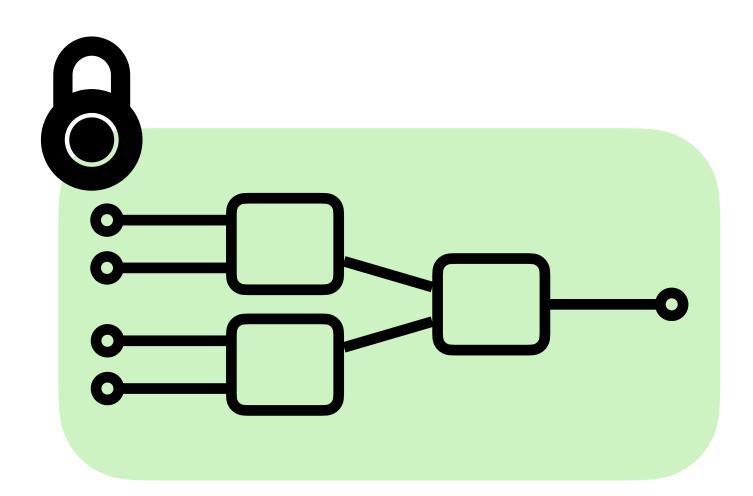
Pseudorandom functions/encryption

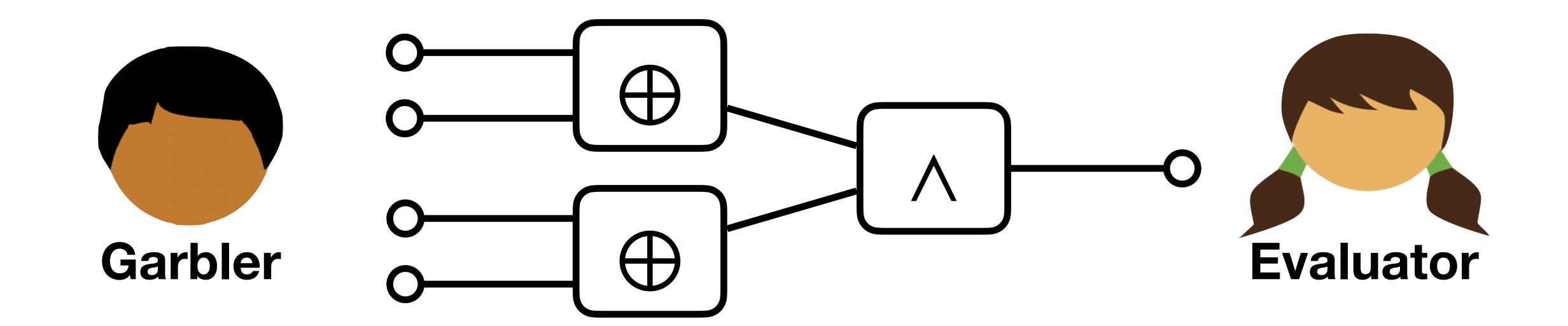
Commitments

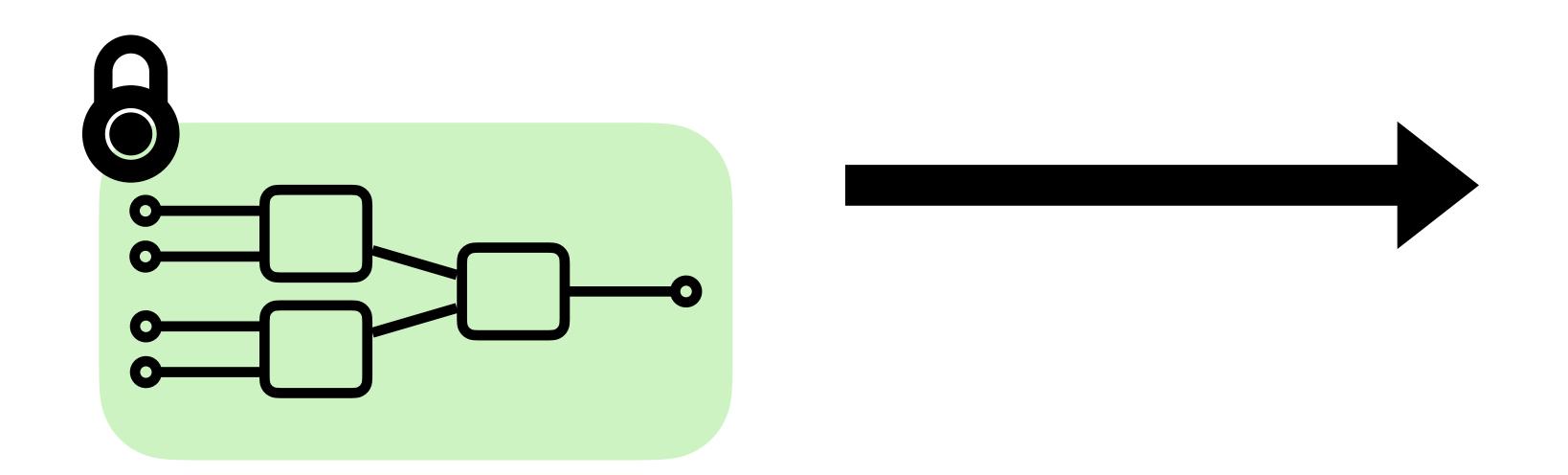
ORAM

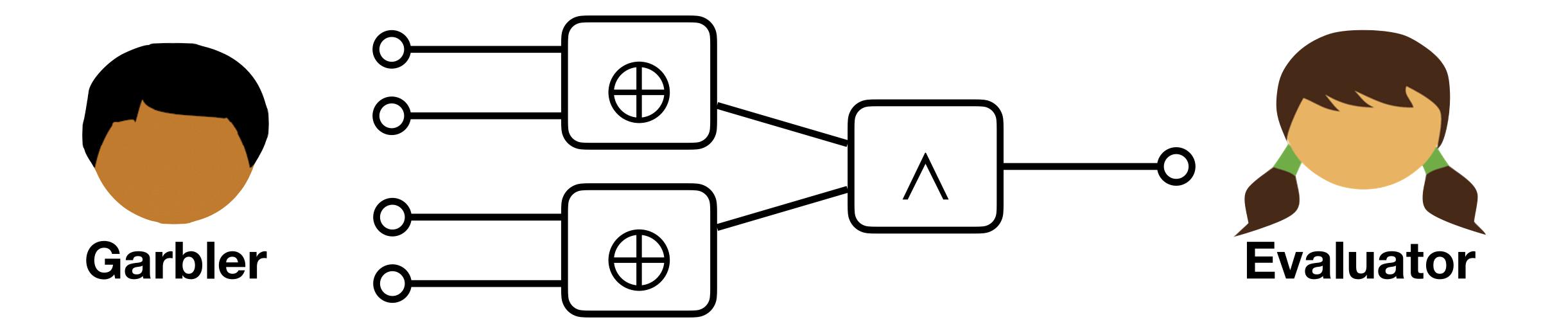


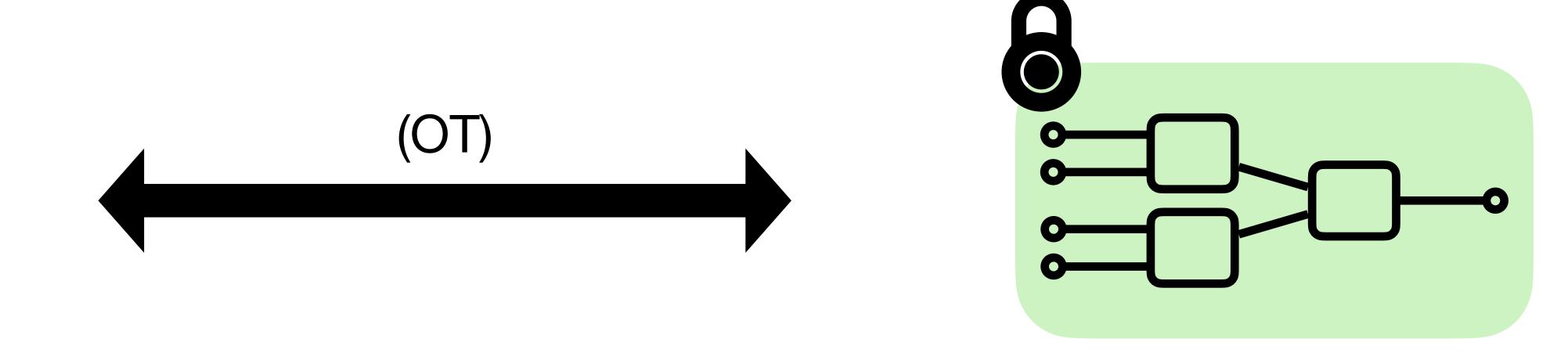


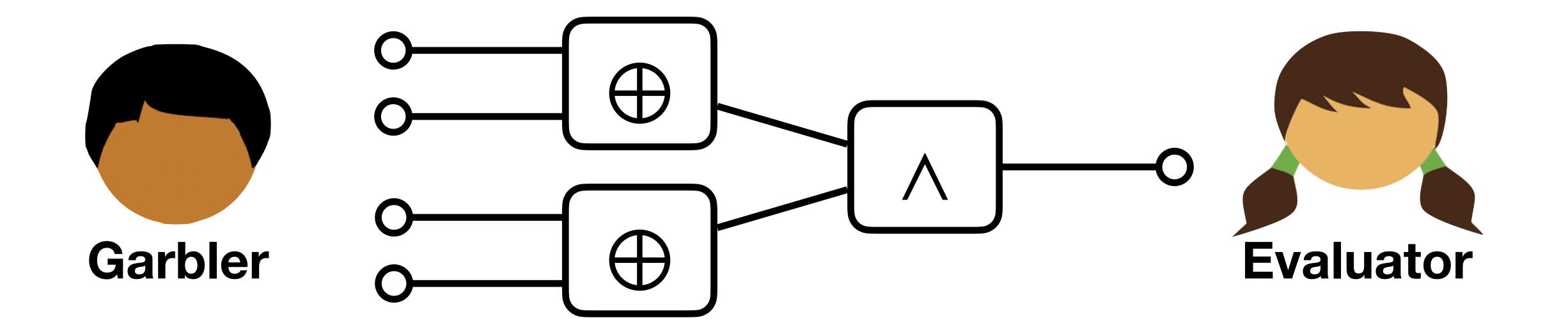


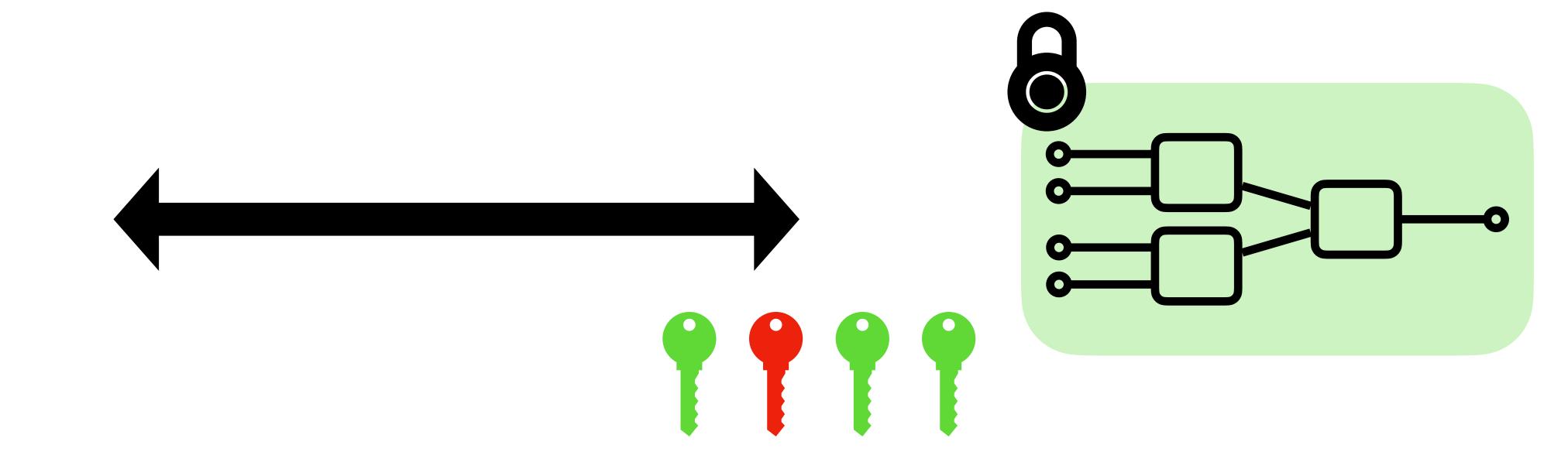


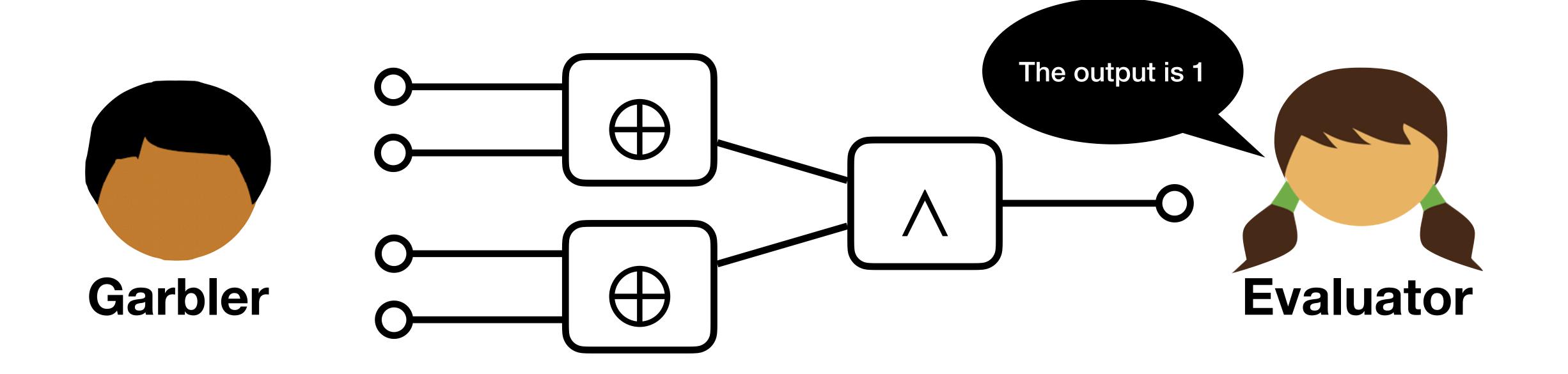


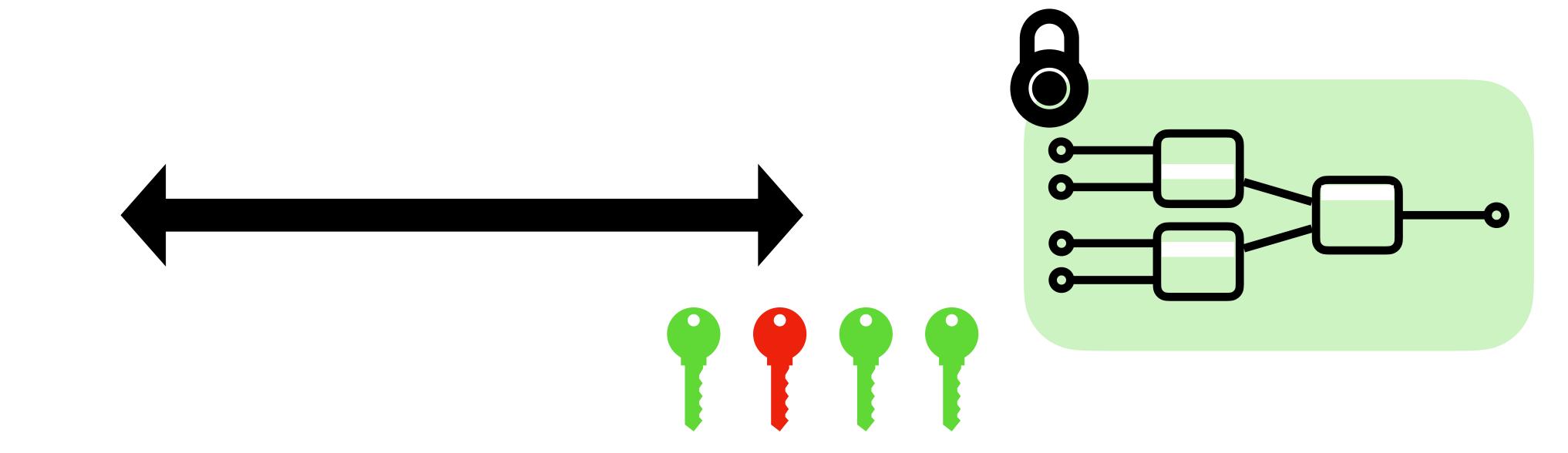




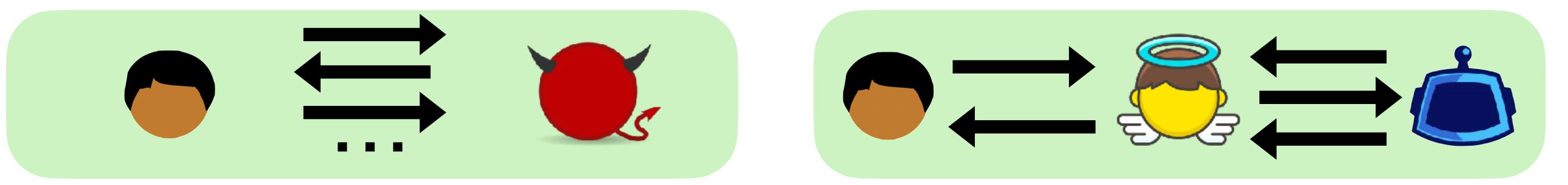






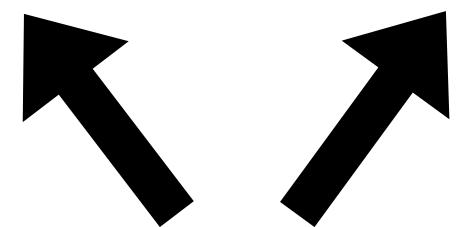


Malicious Security (with abort)



A protocol Π securely realizes a functionality f in the presence of a malicious (with abort) adversary if for **every** real-world adversary \mathscr{A} corrupting party i, **there exists** an ideal-world adversary \mathscr{S}_i (a simulator) such that for all inputs x, y the following holds:

 $\operatorname{Real}_{\mathscr{A}}^{\Pi}(x,y) \approx \operatorname{Ideal}_{\mathscr{S}_i}^f(x,y)$



Ensemble of outputs of each party



 $\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^0,K_c^0))$

 $\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^1,K_c^0))$

 $\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^0,K_c^0))$

 $\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^1,K_c^1))$

Why can't we simulate G?

G can encrypt each gate freely

E has no way to tell if gate it correctly garbled



 $\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^0,K_c^0))$

 $\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^1,K_c^0))$

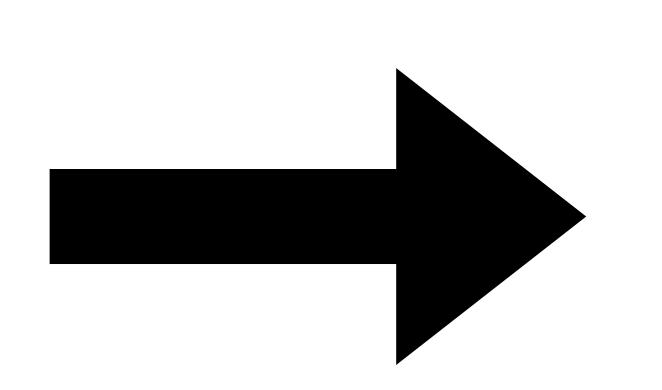
 $\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^0,K_c^0))$

 $\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^1,K_c^1))$

Why can't we simulate G?

G can encrypt each gate freely

E has no way to tell if gate it correctly garbled

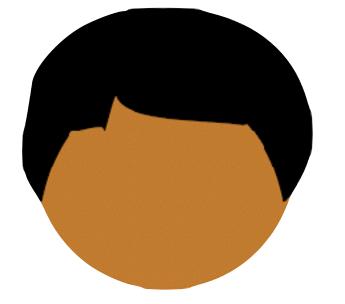


$$\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^0,K_c^0))$$

$$\operatorname{Enc}(K_a^0,\operatorname{Enc}(K_b^1,K_c^0))$$

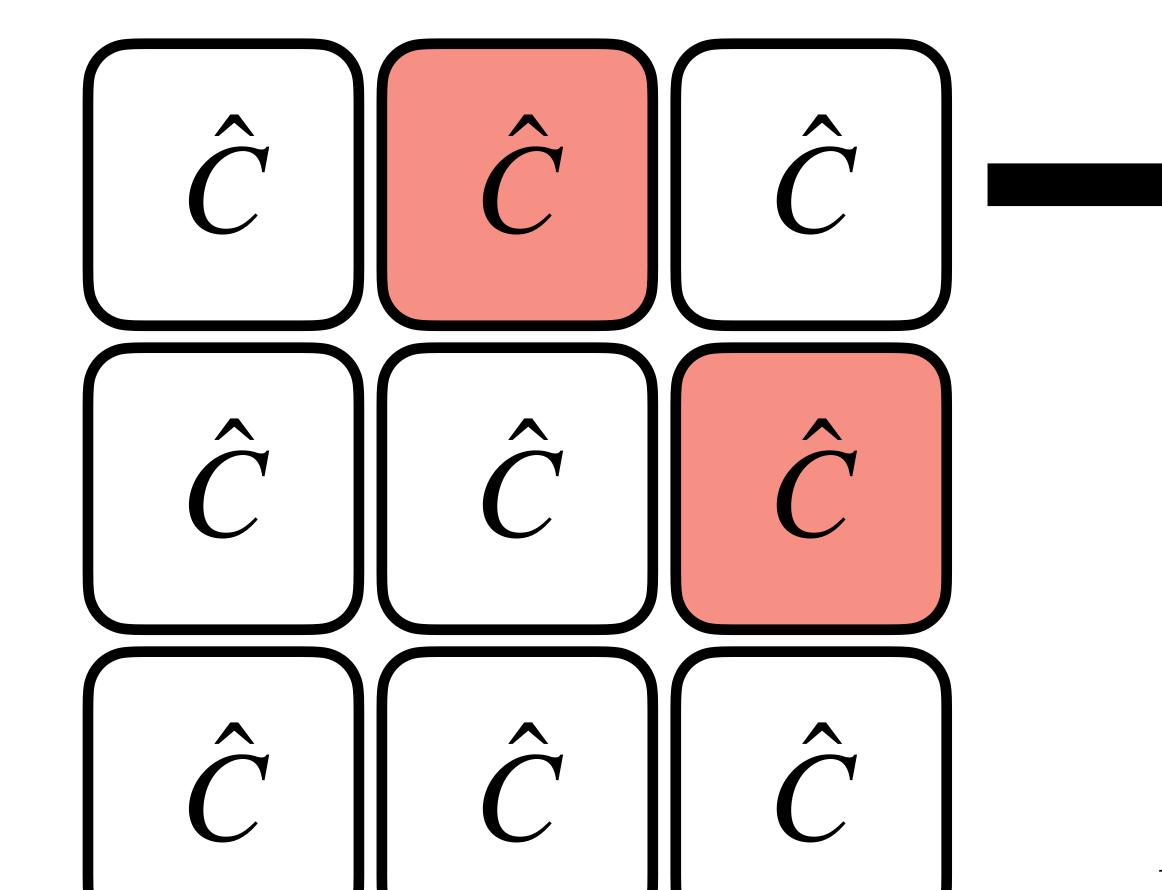
$$\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^0,K_c^1))$$

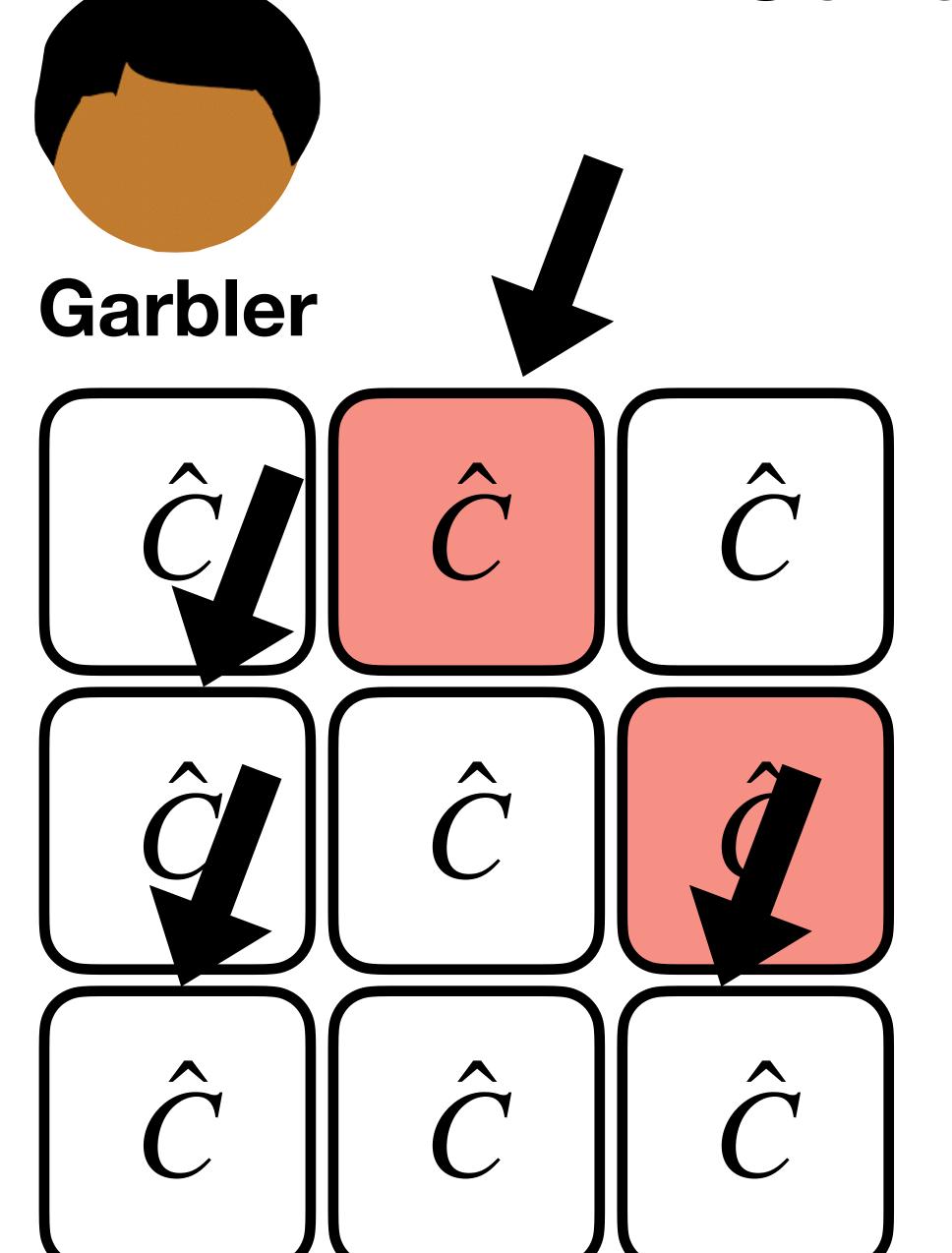
$$\operatorname{Enc}(K_a^1,\operatorname{Enc}(K_b^1,K_c^1))$$





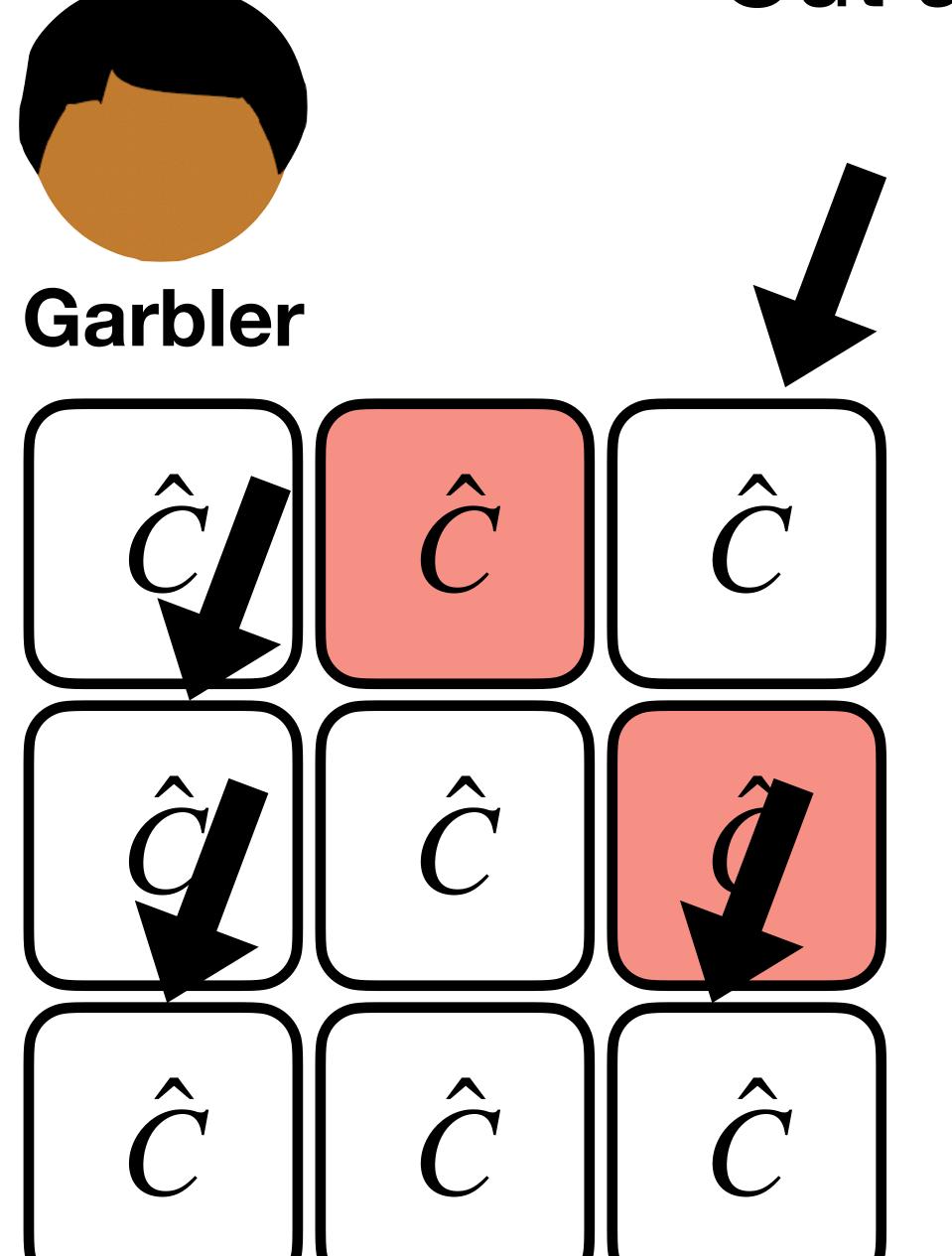








If any opened GC are ill-formed, E aborts

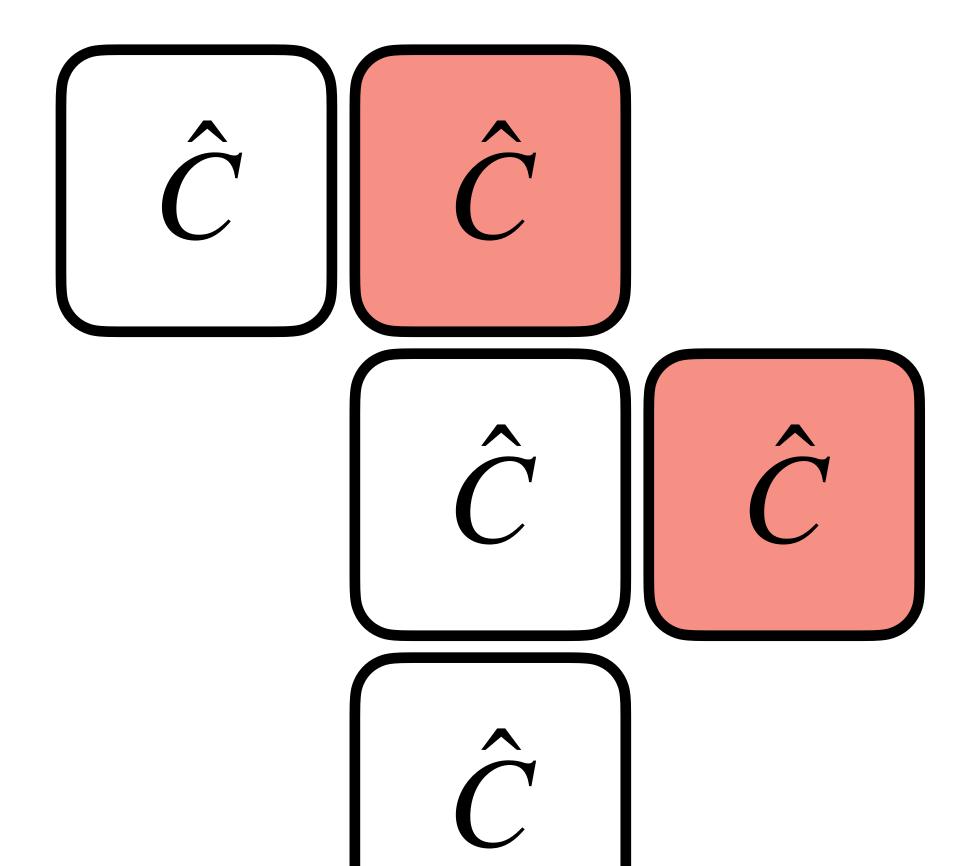




If all opened GC are well-formed, parties continue







Parties evaluate remaining GCs, and E obtains outputs from each GC

Now what?

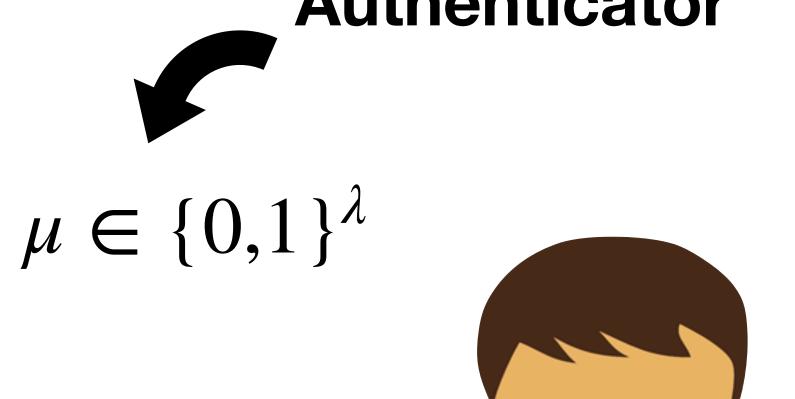
Evaluator takes majority output







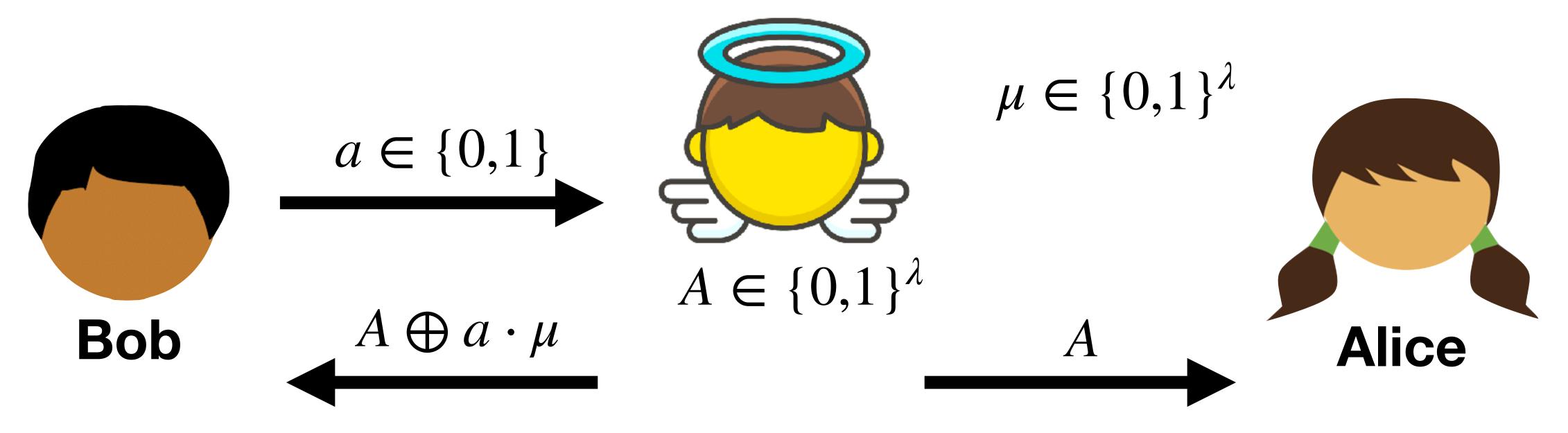
Alice



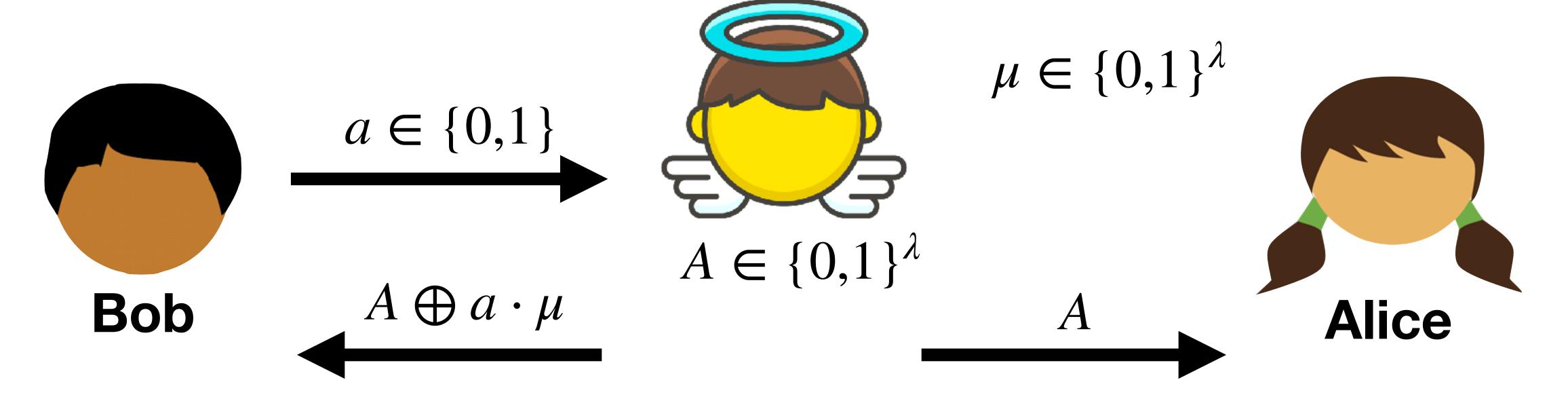
 $a \in \{0,1\}$

Bob

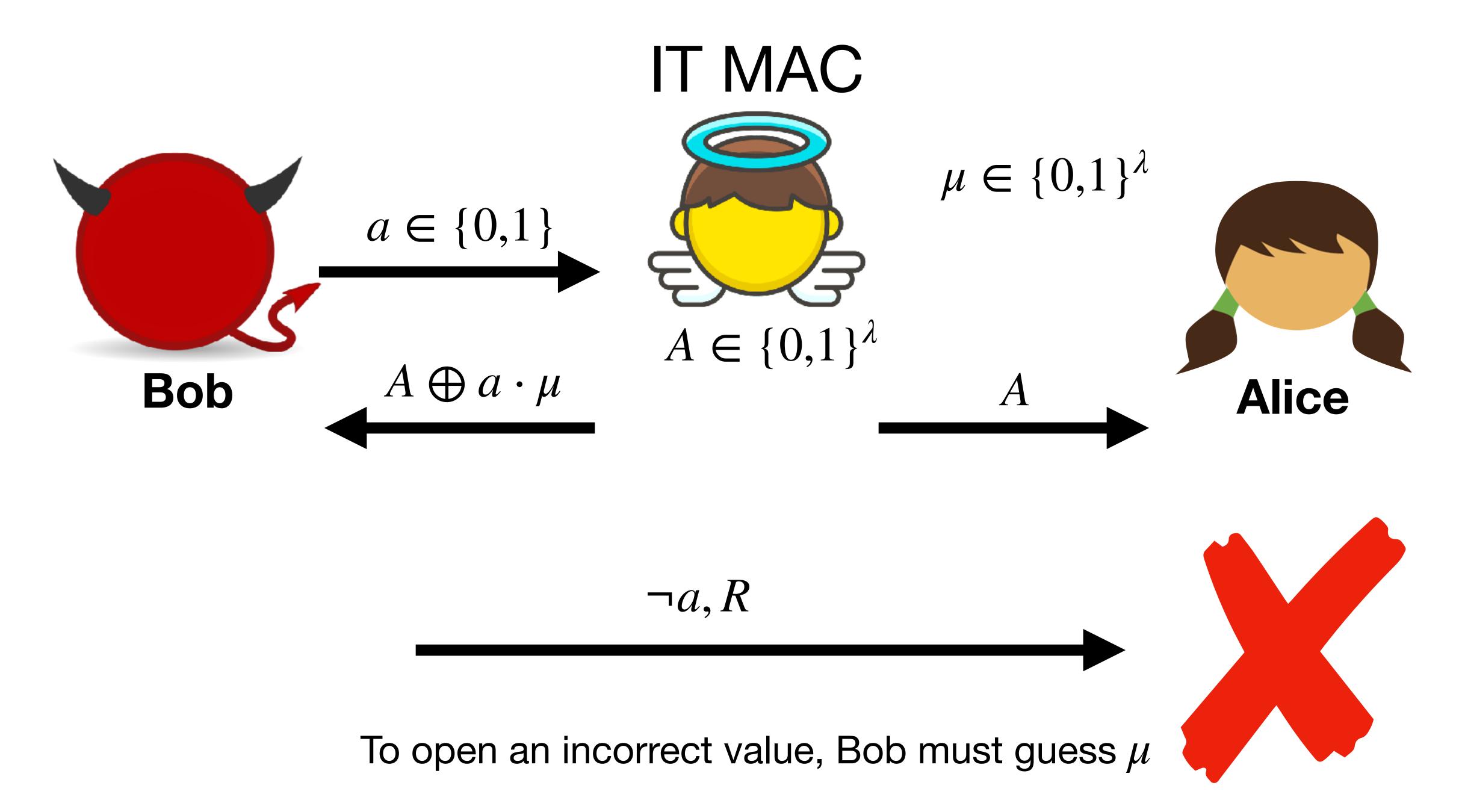
IT MAC

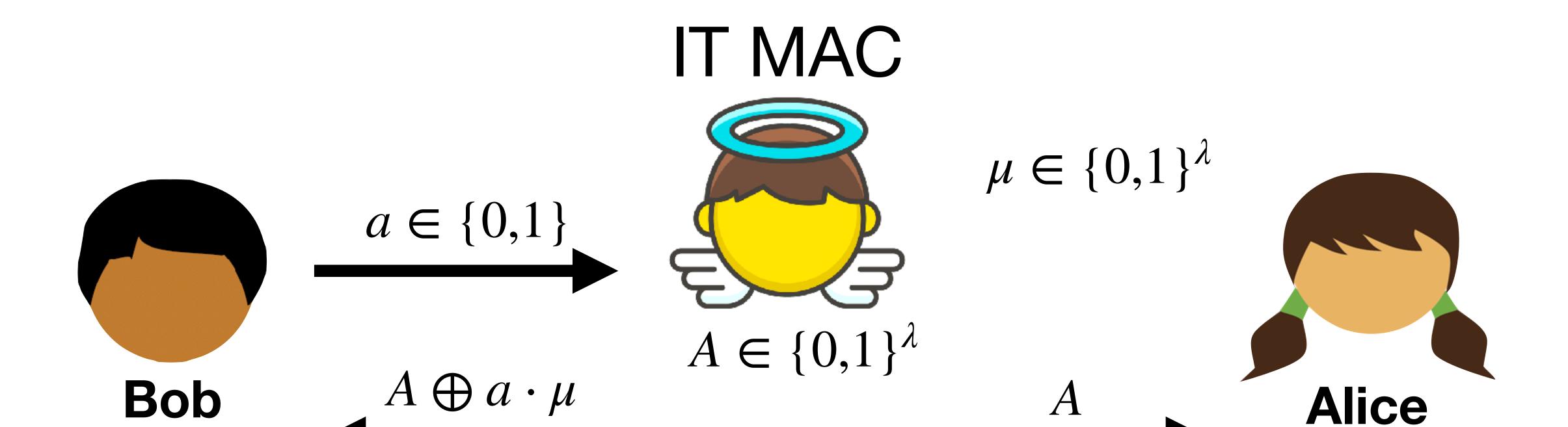


IT MAC



$$a, A \oplus a \cdot \mu$$





$$\langle A \oplus a \cdot \mu, A \rangle \oplus \langle B \oplus b \cdot \mu, B \rangle = \langle (A \oplus B) \oplus (a \oplus b) \cdot \mu, A \oplus B \rangle$$
$$[a \cdot \mu] \oplus [b \cdot \mu] = [(a \oplus b) \cdot \mu]$$

IT MACs are linearly homomorphic

Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation

Xiao Wang University of Maryland wangxiao@cs.und.edu

Samuel Ranellucci University of Maryland George Mason University

samuel@umd.edu

Jonathan Katz University of Maryland jkatz@cs.umd.edu

Abstract

We propose a simple and efficient framework for obtaining efficient constant-round protocols for maliciously secure two-party computation. Our framework uses a function-independent preprocessing phase to generate authenticated information for the two parties; this information is then used to construct a *single* "authenticated" garbled circuit which is transmitted and evaluated.

We also show how to efficiently instantiate the preprocessing phase by designing a highly optimized version of the TinyOT protocol by Nielsen et al. Our overall protocol outperforms existing work in both the single-execution and amortized settings, with or without preprocessing:

- In the single-execution setting, our protocol evaluates an AES circuit with malicious security in 37 ms with an online time of just 1 ms. Previous work with the best online time (also 1 ms) requires 124 ms in total; previous work with the best total time requires 62 ms (with 14 ms online time).
- If we amortize the computation over 1024 executions, each AES computation requires just 6.7 ms
 with roughly the same online time as above. The best previous work in the amortized setting has
 roughly the same total time but does not support function-independent preprocessing.

Our work shows that the performance penalty for maliciously secure two-party computation (as compared to semi-honest security) is much smaller than previously believed.

1 Introduction

Protocols for secure two-party computation (2PC) allow two parties to compute an agreed-upon function of their inputs without revealing anything additional to each other. Although originally viewed as impractical, protocols for generic 2PC in the semi-honest setting based on Yao's garbled-circuit protocol [Yao86] have seen tremendous efficiency improvements over the past several years [MNPS04, HEKM11, ZRE15, KS08, KMR14, ALSZ13, BHKR13, PSSW09].

While these results are impressive, semi-honest security—which assumes that both parties follow the protocol honestly yet may try to learn additional information from the execution—is clearly not sufficient for all applications. This has motivated researchers to construct protocols achieving the stronger notion of malicious security. One popular approach for designing constant-round maliciously secure protocols is to apply the "cut-and-choose" technique [LP07, sS11, sS13, KSS12, LP11, HKE13, Lin13, Bra13, FJN14, AMPR14] to Yao's garbled-circuit protocol. For statistical security $2^{-\rho}$, the best approaches using this paradigm require ρ garbled circuits (which is optimal); the most efficient instantiation of this approach, by Wang et al. [WMK17], securely evaluates an AES circuit in 62 ms.

The cut-and-choose approach incurs significant overhead when large circuits are evaluated precisely because ρ garbled circuits need to be transmitted (typically, $\rho \geq 40$). In order to mitigate this, recent works have explored secure computation in an *amortized* setting where the same function is evaluated multiple times

1

Optimizing Authenticated Garbling for Faster Secure Two-Party Computation

Jonathan Katz University of Maryland jkatz@cs.umd.edu Samuel Ranellucci
University of Maryland
George Mason University
samuel@und.edu

Mike Rosulek
Oregon State University
rosulekm@eecs.oregonstate.edu

Xiao Wang University of Maryland vangxiao@cs.umd.edu

October 10, 2018

Authenticated Garbling from Simple Correlations

Samuel Dittmer $^{1[0000-0003-0018-6354]}$, Yuval Ishai 2 , Steve Lu $^{1[0000-0003-1837-8864]}$, and Rafail Ostrovsky $^{1,3[0000-0002-1501-1330]}$

- Stealth Software Technologies, Inc.
- ² Technion Israel Institute of Technology
- ³ University of California, Los Angeles

Abstract. We revisit the problem of constant-round malicious secure two-party computation by considering the use of *simple correlations*, namely sources of correlated randomness that can be securely generated with sublinear communication complexity and good concrete efficiency. The current state-of-the-art protocol of Katz et al. (Crypto 2018) achieves malicious security by realizing a variant of the *authenticated garbling* functionality of Wang et al. (CCS 2017). Given oblivious transfer correlations, the communication cost of this protocol (with 40 bits of statistical security) is comparable to roughly 10 garbled circuits (GCs). This protocol inherently requires more than 2 rounds of interaction.

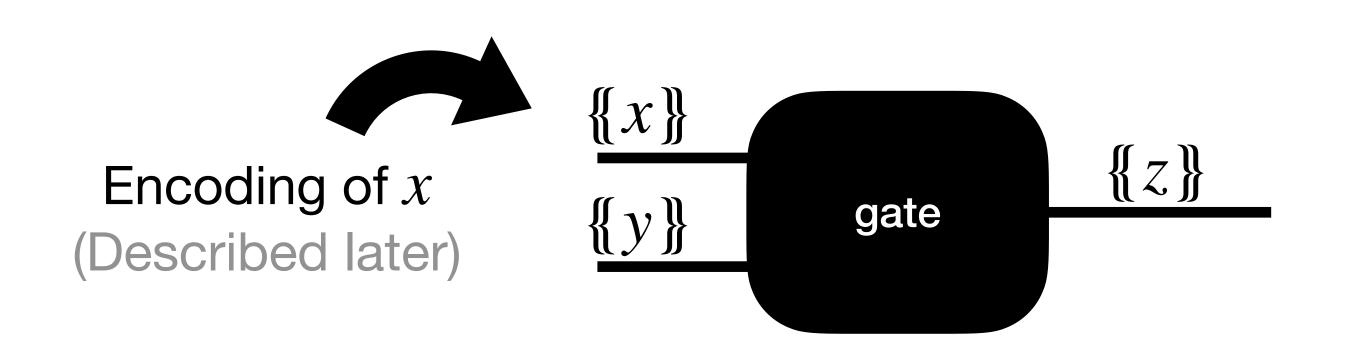
In this work, we use other kinds of simple correlations to realize the authenticated garbling functionality with better efficiency. Concretely, we get the following reduced costs in the random oracle model:

- Using variants of both vector oblivious linear evaluation (VOLE) and multiplication triples (MT), we reduce the cost to 1.31 GCs.
- Using only variants of VOLE, we reduce the cost to 2.25 GCs.
- Using only variants of MT, we obtain a non-interactive (i.e., 2-message) protocol with cost comparable to 8 GCs.

Finally, we show that by using recent constructions of pseudorandom correlation generators (Boyle et al., CCS 2018, Crypto 2019, 2020), the simple correlations consumed by our protocols can be securely realized without forming an efficiency bottleneck.

T . 1 ..

Crucial Insight: use information-theoretic MACs on each wire so that GC can reveal internal values to E. E can tell if a the revealed value is corrupted.

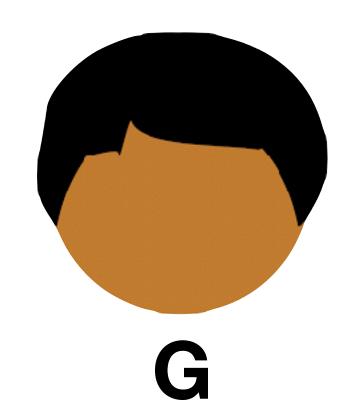


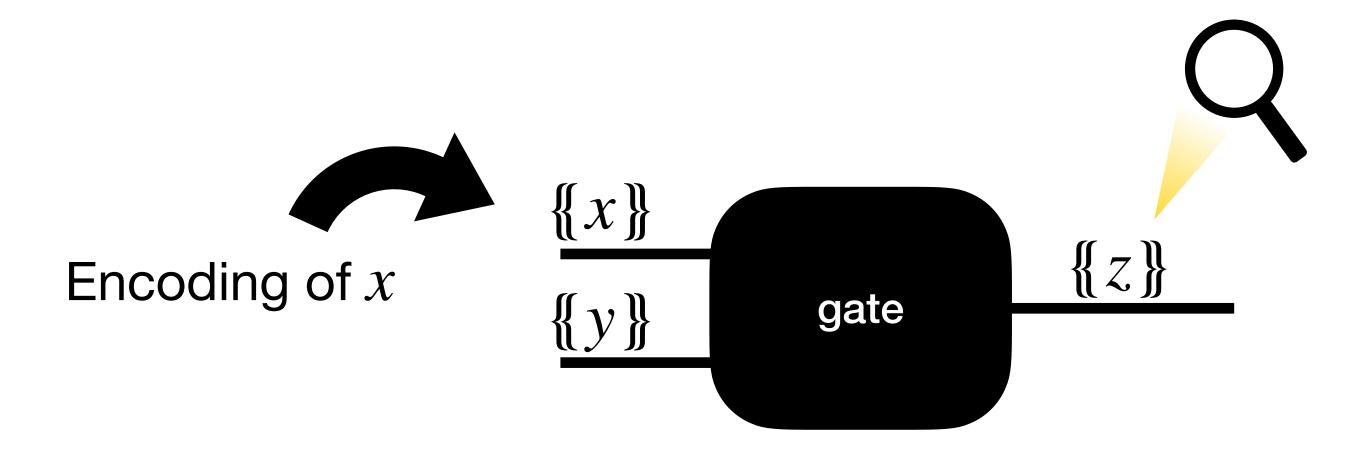
Just like classic GC, gate-by-gate evaluation in constant rounds



However, the technique prevents G from cheating

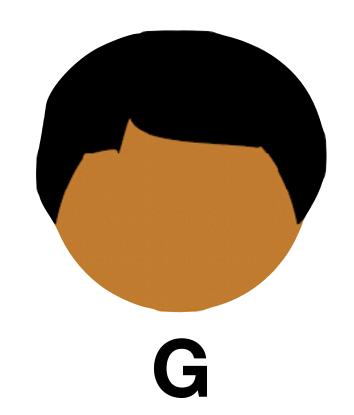
Crucial Insight: add a mechanism by GC can reveal internal values to E. E can tell if a the revealed value is corrupted.

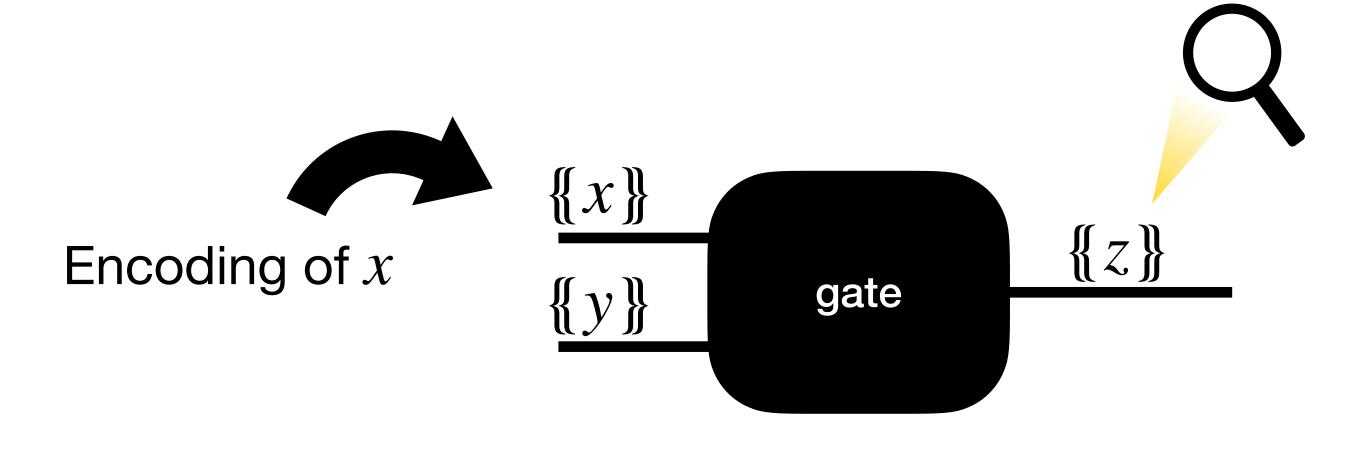


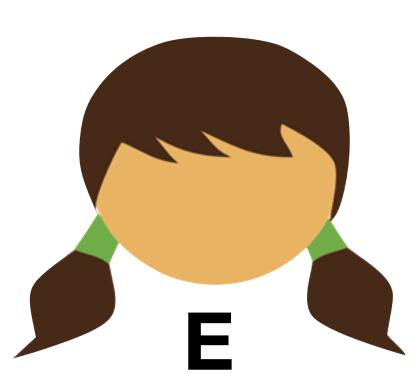




Crucial Insight: add a mechanism by GC can reveal internal values to E. E can tell if a the revealed value is corrupted.



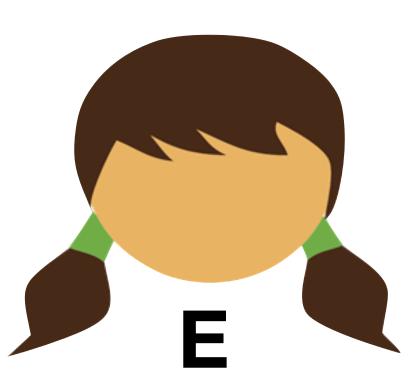




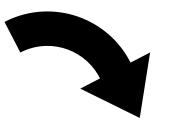
If G tries to corrupt the GC, then E will notice z is ill-formed with overwhelming probability

 $\{x\}$

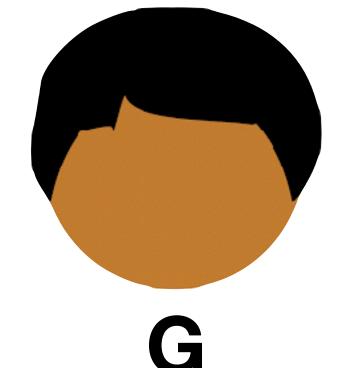




Key



$$\Delta \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$



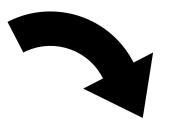
 $\{\!\!\{ \boldsymbol{\mathcal{X}} \}\!\!\}$

Authenticator

$$\mu \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$



Key

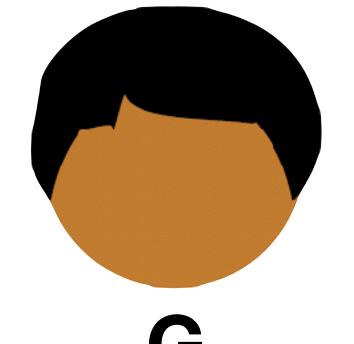


$$\Delta \leftarrow \{0,1\}^{\lambda}$$

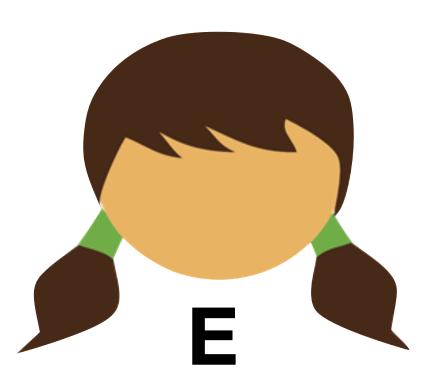
{{ X }}



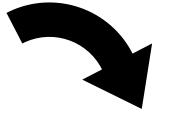
$$\mu \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$



$$\{\!\!\{x\}\!\!\} = \left\langle X, \left\{\begin{matrix} X & \text{if } x = 0 \\ X \oplus (\Delta, \mu, 1) & \text{if } x = 1 \end{matrix} \right\}$$



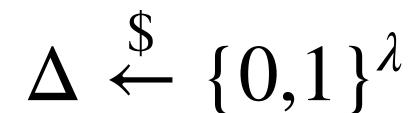
Key

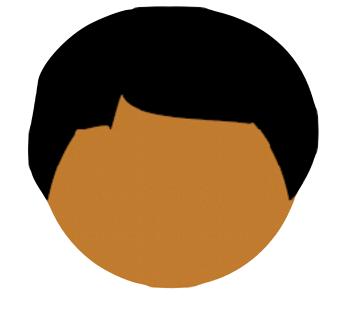


$$\{\!\{x\}\!\}$$

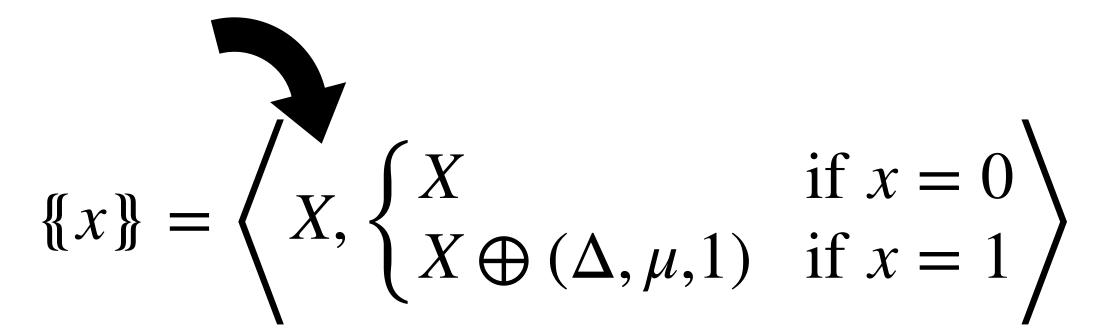
Authenticator

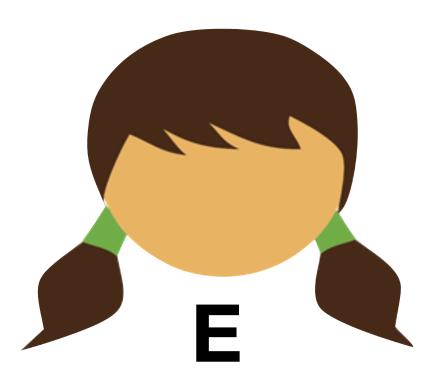
$$\mu \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$



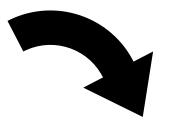


$$X \in \{0,1\}^{2\lambda+1}$$





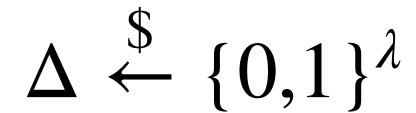
Key

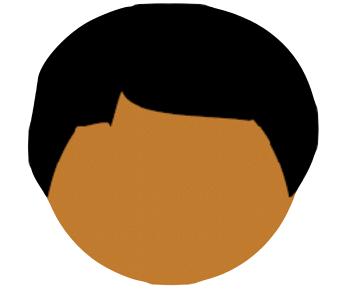


$$\{\!\{X\}\!\}$$

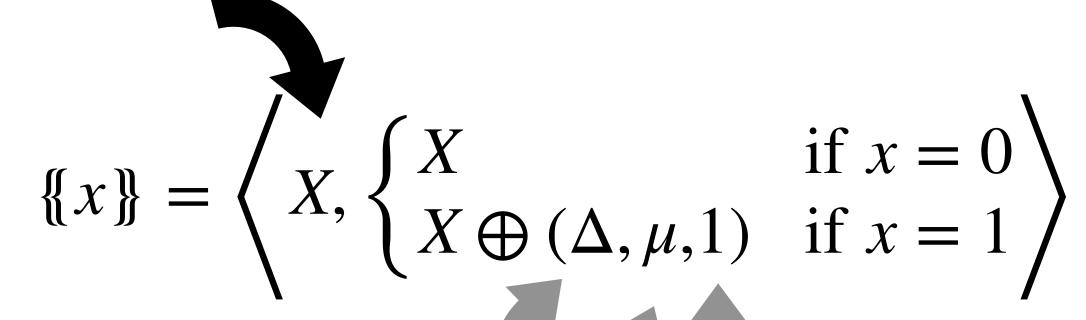
Authenticator

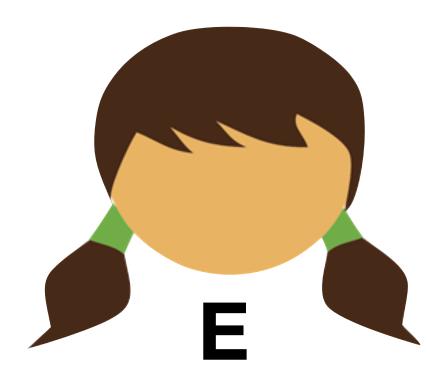
$$\mu \leftarrow \{0,1\}^{\sigma}$$





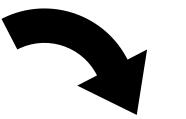
$$X \in \{0,1\}^{2\lambda+1}$$







Key

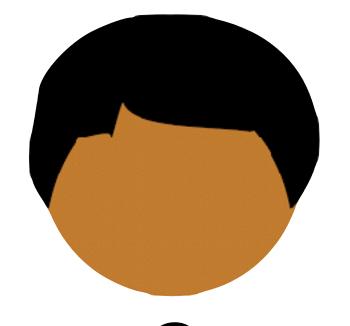


$$\Delta \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$

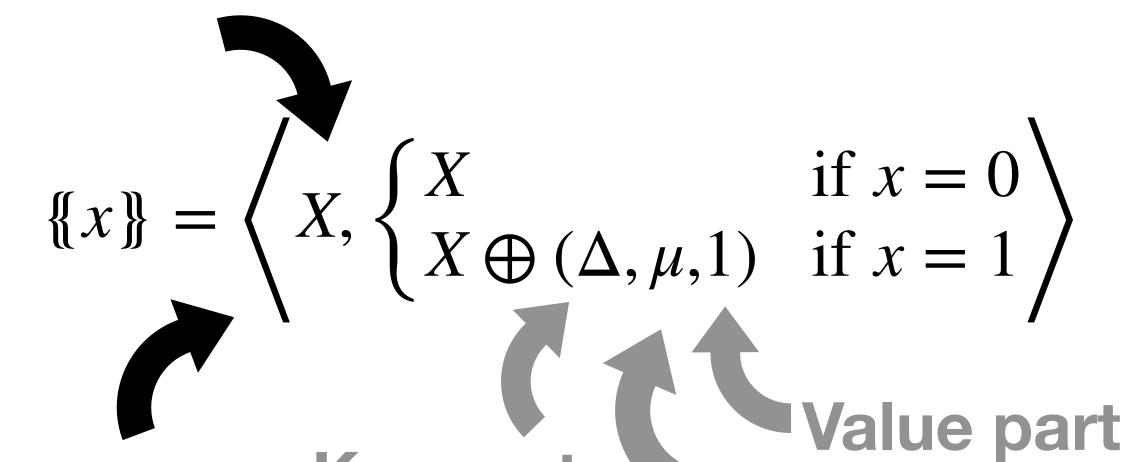


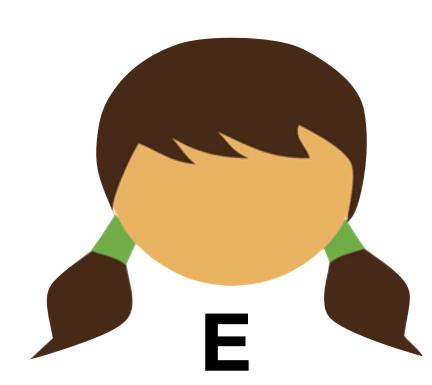


$$\mu \stackrel{\$}{\leftarrow} \{0,1\}^{\sigma}$$



$$X \in \{0,1\}^{2\lambda+1}$$

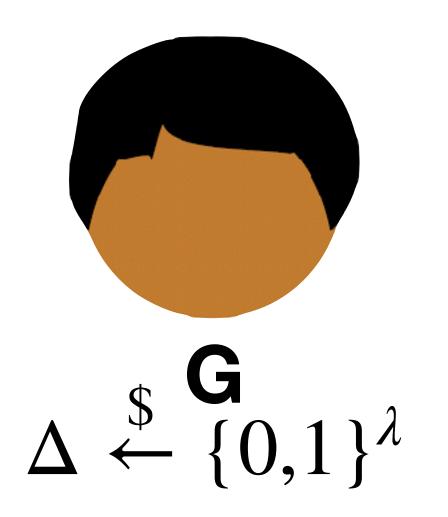




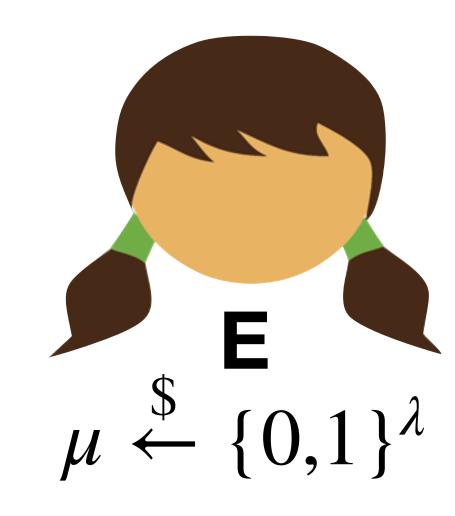
Secret-share of parts

Key part Authenticator part

$$\{\!\!\{x\}\!\!\} = [x \cdot \Delta, x \cdot \mu, x]$$



$$\{x\} = \left\langle X, \begin{cases} X & \text{if } x = 0 \\ X \oplus (\Delta, \mu, 1) & \text{if } x = 1 \end{cases} \right\rangle$$
Key part
Authenticator part



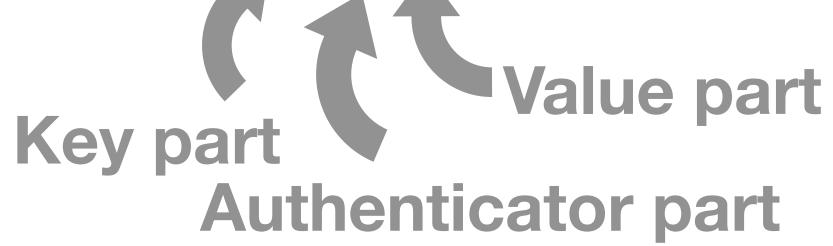
$$\{\!\!\{x\}\!\!\} = [x \cdot \Delta, x \cdot \mu, x]$$

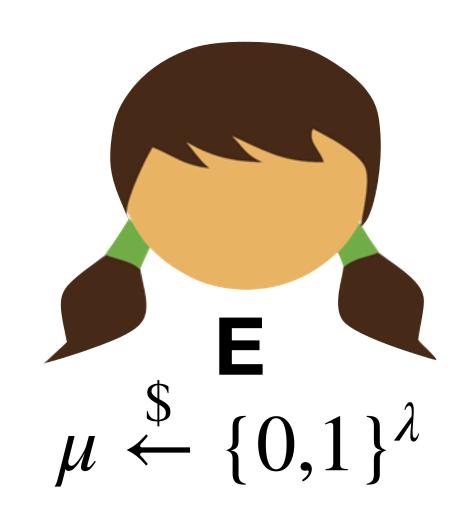
open authenticator, value

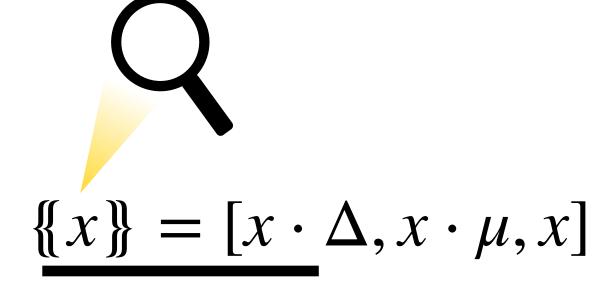
$$x \cdot \mu, x$$

$$\Delta \leftarrow \{0,1\}^{\lambda}$$

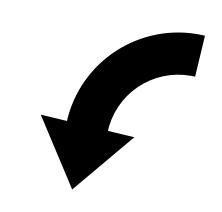
$$\{\!\!\{x\}\!\!\} = \left\langle X, \left\{ \begin{matrix} X & \text{if } x = 0 \\ X \oplus (\Delta, \mu, 1) & \text{if } x = 1 \end{matrix} \right. \right\rangle$$







open authenticator, value



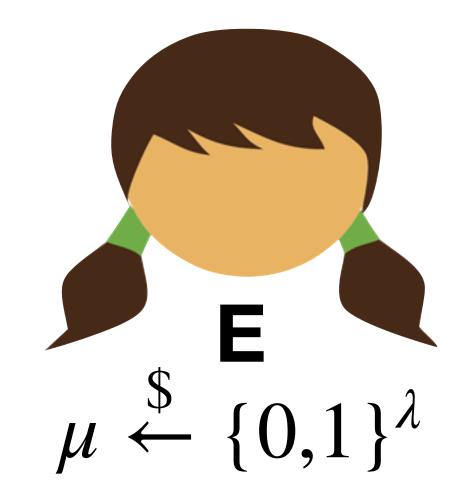
 $x \cdot \mu, x$

G cannot flip bit, because G does not know μ

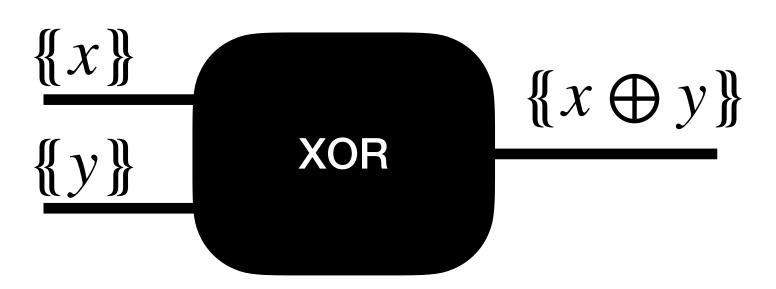


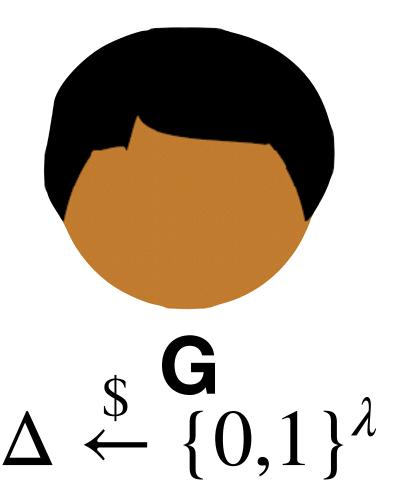
$$\{\!\!\{x\}\!\!\} = \left\langle X, \left\{ \begin{matrix} X & \text{if } x = 0 \\ X \oplus (\Delta, \mu, 1) & \text{if } x = 1 \end{matrix} \right. \right\rangle$$



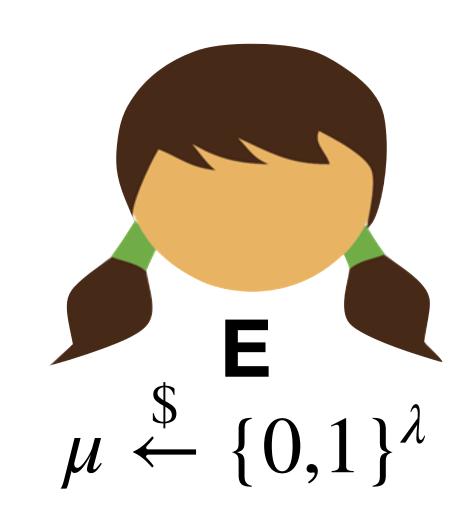


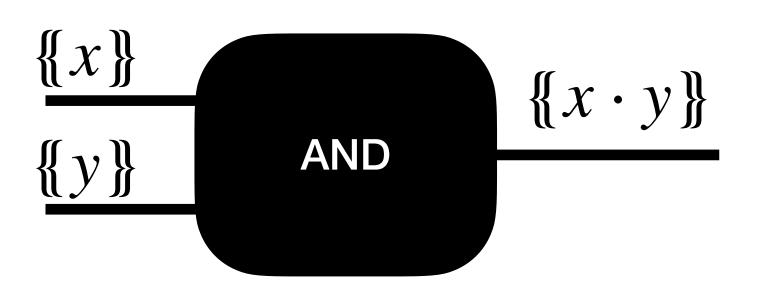
XOR gates are "free"

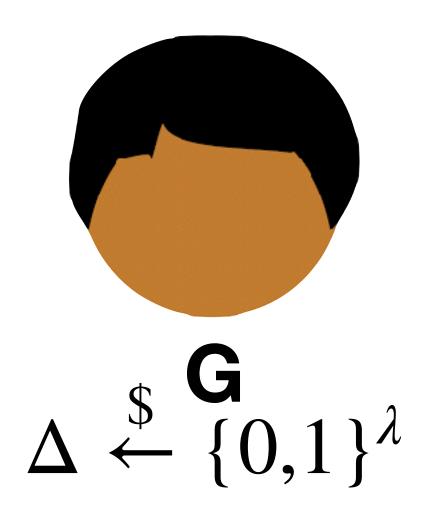




$$\{ \{x\} \} = [x \cdot \Delta, x \cdot \mu, x]$$
$$\{ \{y\} \} = [y \cdot \Delta, y \cdot \mu, y]$$
$$\{ \{x \oplus y\} \} = [(x \oplus y) \cdot \Delta, (x \oplus y) \cdot \mu, (x \oplus y)]$$

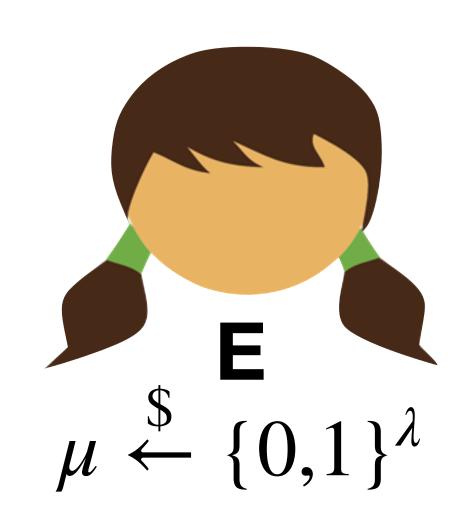






Suppose G and E have access to a doubly authenticated multiplication triple

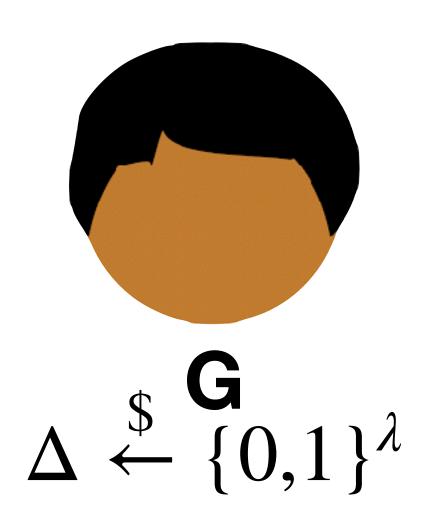
$$\{\{\alpha\}, \{\{\beta\}\}, \{\{\alpha\cdot\beta\}\}\}$$
where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$



$$\{\{\alpha\},\{\{\beta\}\},\{\{\alpha\cdot\beta\}\},\{\{x\}\},\{\{y\}\}\}$$

where
$$\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$$

Observe:
$$(x \oplus \alpha) \cdot y \oplus (y \oplus \beta) \cdot \alpha \oplus \alpha \cdot \beta = x \cdot y$$



In 34th Euroceput, Sofia, Eulgaria, April 2315

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Haif Gates

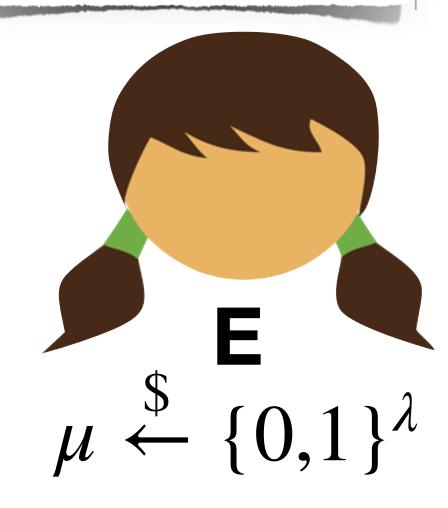
Samee Zahur, Mille Rosulek, and David Evens

Programment of Virginia (someo,evans) @Virginia.edu
Divgen Save University museknopteeck pregonative ad

Abstract. The well-hower viscoled constructions of public viscolits are first eligibrated; per gate, although rations methods have been proposed to reduce this cost. The best previously known methods for optimizing AND gates (we explorated): Pools and A. SALGENET 1009; and XOR gates three ripherentic Ecolosities and Schneider, ECALE 2009 west incompatible, so meetinglementations used the best known method compatible with fine-KOR gates (three explorated): Recessitive and Schneider, ECALE 2008; in this work we show how to simultaneously garble AND gates using two eightestests and KOR gates using acrossphericus, straining in smaller public disturbs than any griter scheme. The main bits abhide was contained and almost gates are help gates. AND gates for which one pury known one input. Each half-gate cambe garbled with a single diphereou, so our constanction one we eightertons for each AND gate while being compatible with look XCR gates. The price for the relaction in size in that the evaluator state perform two cryptographic operations per AND gate, rather framework in previous releases. We experimentally demonstrate for or subtruly selected that our construction is not rather than the construction is not and the analysis of the properties application. We show that our construction is not and the almost or pathing schemes we compacting all known practical garding voluntypes.

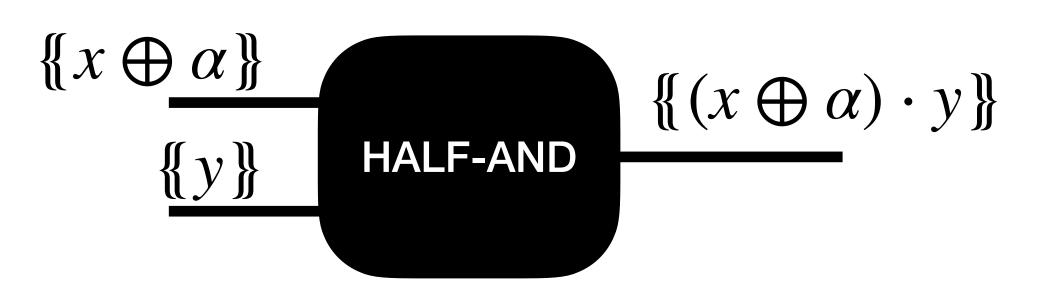
1 Introduction

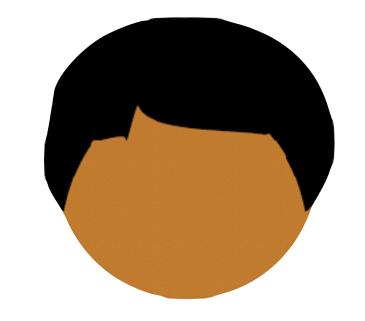
Yea's garbled direat; exhitique remains one of the mess promiting and actively moded methods for secuse multi-party computation. The first implementation of secuse two-party computation (2PC) [26] used Yan's basic garbled circuit approach, and internains the primary (but not entry) paradigm for the many 2PC implementation that have been developed over the past ten years [25, 26, 18, 14, 21, 12]. Because the generation and execution of gates beastise from advances in processor speed (in pasticular, hardware supportferery/stographic operation) as well as the increasing availability of large numbers of evera, the computation time and cost for garbled circuit protocels has dropped demantically. Thus, the main bottleneck for 2PC protoceds is network bandwidth which is predominantly due to the transmission of garbled gates. Many optimizations in 2PC have focused on activating the size of the garbled circuits themselves [27,20, 19] and achieving the number of circuits required (in the case of multi-less occurity) [24, 29, 21, 15, 6] Curvaric reduces the curvail size of garbled circuits by reducing the amount of data that avoids to be transferred for each garbled gate.



$$\{\{\alpha\}, \{\{\beta\}\}, \{\{\alpha \cdot \beta\}\}, \{\{x\}\}, \{\{y\}\}\}$$

where
$$\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$$





$$\Delta \stackrel{\$}{\leftarrow} \mathbf{G}$$

$$\Delta \leftarrow \{0,1\}^{\lambda}$$

In 34th Euroceypt, Sofia, Eulgaria, April 2015

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Haif Gates

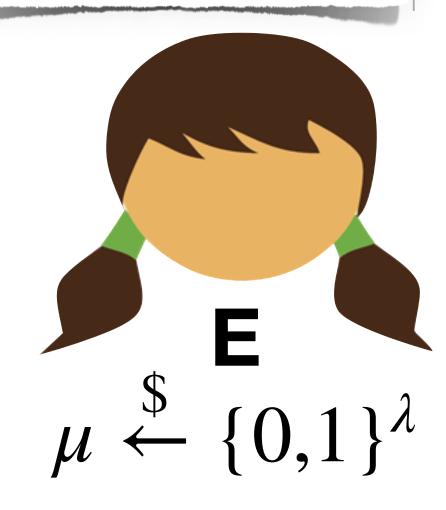
Samee Zahur, Milit Rosulek, and David Evans

http://kightset-viccon/nargates University of Virginia (sames, event) @virginia.edu Drogen State Delevraty misseknopeecs.psegonstee ed

Abor wit. The well-harwen visuoical constructions of publical vironits use fiver eighesteets per gate, although surious methods have been proposed to reduce this cost. The best previously known methods for optimizing AND gates (not eighesteet). Perkins et al., ASIACONFT 1000) and XDO gates three eighesteets: Eclestrikes and Schneider, ECALP 2003) were inconousliste, to meet implementations used the best known method compatible with five-XOR gates (have eightesteet). Rotestakes and Schneider, ECALP 2003). In this work we show how to simultaneously garble AND gates using two eightesteets and XOR gates using two eightesteets and XOR gates using two exploritests, resulting in smaller garbled circuits than any grow scheme. The main likes behind we construction in the local and XOR gates into morbell/gasts — AND gates for which one pury knows one input. Each half-gate can be garbled with a single eighterest, so our communities near two eighterests for each AND gate while being compatible with local XOR gates. The price for the reduction in size is that the evaluator mass perform two exprographic operations or AND gate rather functions in previous colorums. We also generately a sequence by a color of arbitrag schemes who companies all learners procedured gateling techniques.

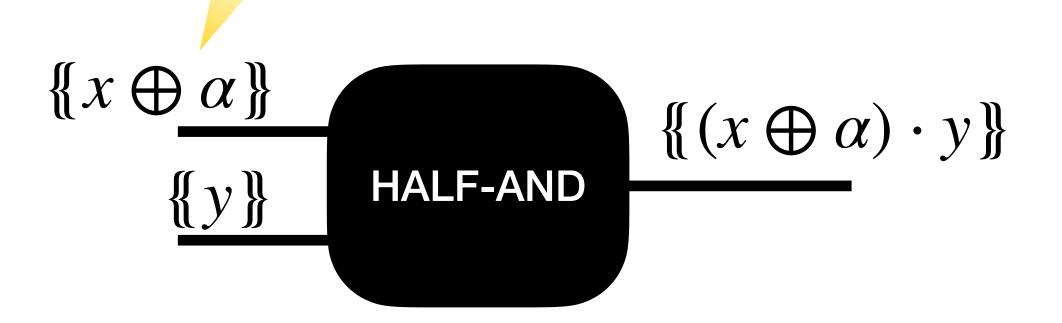
1 Introduction

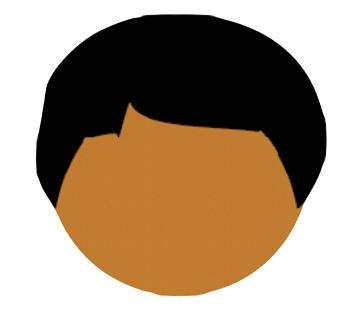
Yao's garbled circuit technique remains one of the mess promising and actively studied methods for secuse multi-party computation. The first implementation of secuse two-party computation (19C) [36] used Yao's basic gashied circuit approach, and internation the primary (but not only) paradigm for the many 2PC implementation that have been developed over the past ten years [25, 26, 10, 14, 21, 12]. Because the generation and execution of gasts benefits from advances in processor speed (in graticular, hardware supportfacery) togenphic operation!) as well as the internating resimilarity of large numbers of evers, the computation time and cost for garbled circuit protocols has dropped demantically. Thus, the main bottleneck for 3PC proceeds is network bundwidth which is predominantly due to the transmission of garbled gases. Many eptimizations in 2PC have bounded on soluting the size of the garbled circuits themselves [27, 20, 19] and addening the number of circuits required (in the case of multi-less sociality) [24, 20, 22, 13, 6]. Currunds reduces the overall size of garbled circuits by reducing the amount of data that needs to be transferred for each garbled gase.



$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}, \{\!\{x\}\!\}, \{\!\{y\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





$$\Delta \leftarrow \{0,1\}^{\lambda}$$

$$\langle X, X \oplus x \cdot \Delta \rangle = \text{keyPart}(\{\{x \oplus \alpha\}\})$$

 $\langle Y, Y \oplus y \cdot (\Delta, \mu, 1) \rangle = \{\{y\}\}$

In 34th Euroceppt, Sofia, Eulgaria, April 2315

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Half Gates

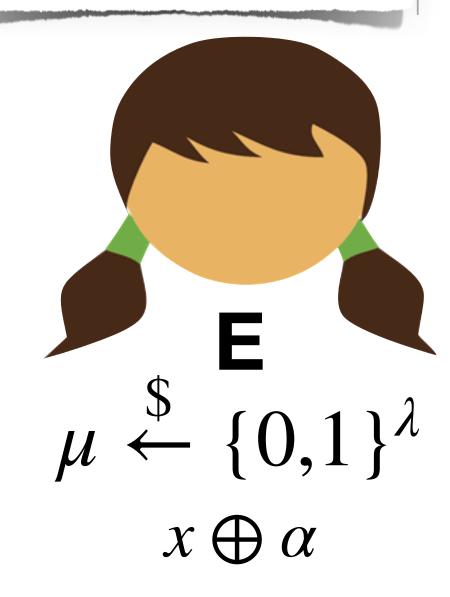
Samee Zahur, Nitte Rosulek, and David Evan

University of Virginia (somes, evans) @virgin Orone State University (\$1,000 per \$1,000 per \$1,000

Abstract. The well-known visionical constructions of publical views in one face algorithms; per gate, although rations methods have been proposed to reduce the cost. The best previously known methods for optimizing AND gates (now explorater). Perform et al., ASLICENETY 1009) and XOB gates (now explorater). Editorithm and Schneider, EALLY 2003) were incorrousline, as meet implementations used the best known method compatible with flor-KOB gates (here explorater). Redestation and Schneider, EALLY 2003, in this work we show those to invaluance only gards. AND pates using two siphoteness and KOB gates using zero explorations, treating in smaller pathod or care in humany prior scheme. The main little whicher was constructions the band on AND gate in the mortality gates. AND gates with a single eligibration, so our communication tensive, eligibration for each AND gate with the being compatible with loss XOB gates. The paint for the recention in size is that the evaluator must perform two exprographic operations per AND gate rather flux occurs in previous schemes. We experimentally demonstrate that our particular strengths and house in previous schemes. We experimentally demonstrate that our gatemps scheme leads to anoverant accurate mine cap to UPA), and image use (up to 2014) over accord benchmark applications. We show that our construction is optimal to a large cause of pathing schemes we companying all learness up accurate pathings.

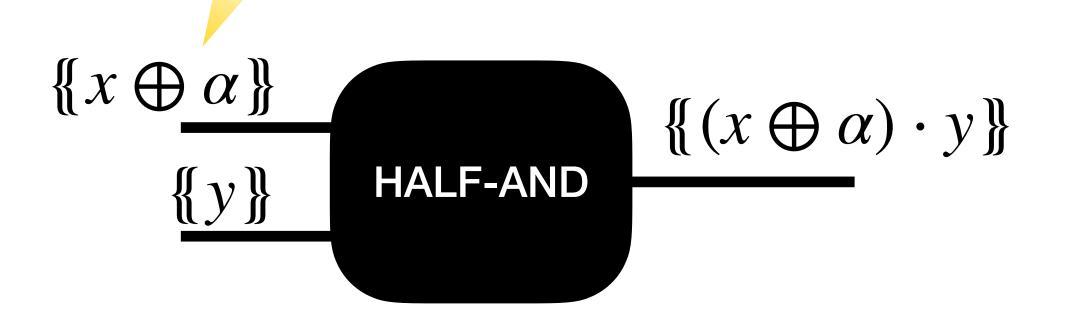
1 Introduction

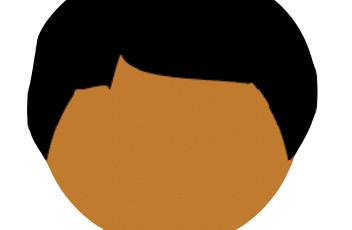
Yea's garbled circuit technique remains one of the most promiting and actively moded methods for secure model party computation. The first implementation of secure two-party computation (3PC) [26] used Yan's basic garbled circuit approach, and iteramins the primary (but moverly) paradigm for the many 2PC implementations that have been developed over the past ten years [25, 26, 18, 14, 21, 12]. Because the generation and execution of gates beastiful from advances in processor speed (in particular, hardware support for cryptographic operations) as well as the increasing restinguishing of large numbers of secus, the computation time and cost for garbled circuit protocels has deeped distributely. Thus, the main botherack for 2PC protocels is network bandwidth which is predominantly due to the transmission of particul gates. Many optimizations in 2PC have focused on soluting the size of the garbled circuits themselves [27, 20, 19] and achoing the number of circuits required (in the case of malicious secusity) [24, 20, 22, 15, 16]. Our wards reduces the coverall some of gathted circuits by reducing the amount of data that weeks to be transferred for each garbled gate.



$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}, \{\!\{x\}\!\}, \{\!\{y\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





$$\Delta \leftarrow \{0,1\}^{\lambda}$$

$$\langle X, X \oplus x \cdot \Delta \rangle = \text{keyPart}(\{\{x \oplus \alpha\}\})$$

 $\langle Y, Y \oplus y \cdot (\Delta, \mu, 1) \rangle = \{\{y\}\}$

Enc(X, Z)

 $\operatorname{Enc}(X \oplus \Delta, Y \oplus Z)$

In 34th Euroceyps, Sofia, Eulgaria, April 2015

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Half Gates

Samee Zahur, Nabe Rosulek, and David Eva

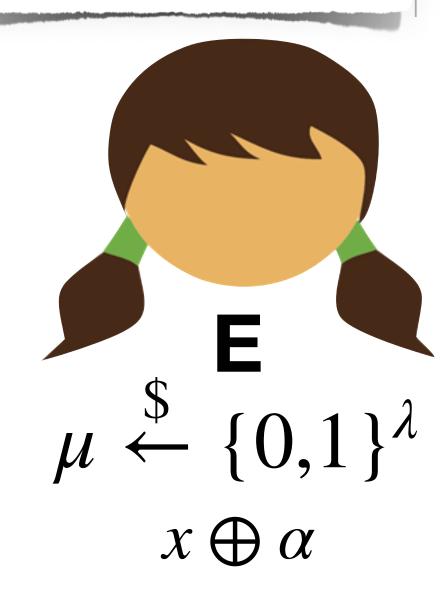
Into::Nightset:vilcommargates University of Virginia (sames, evans) @virginia.

Abstract. The well-known classical constructions of public circuits are four eligiberhest; per gate, although nations methods have been proposed to reduce the cost. The best proviously known methods for optimizing AND gates (two eligiberator). Parks of al., ASLICERFY 1009) and XOB gates (two eligiberator). Parks of al., ASLICERFY 1009) and XOB gates (two eligiberatoris used the best known method compatible with flor-KOB gates (three eligiberatoris would be best known method compatible with flor-KOB gates (two eligiberatoris Kodesmico and Schmeider, ECALP 2008). In this work we show how to simultaneously garlis. AND gates using two eliphorators and KOB gates using zero eliphorator, stretching its smaller garlind circuits than any prior scheme. The main lifes which may construction in broad on AND gate into mortally gater.

AND gates for which may garry known one imput. Each half-gate can be garlied with a single eliphorator, so our construction sensions ever eliphorator for each AND gate with the being compatible with loos. XOB gates. The prior for the recursion in size is that the evaluator must perform two ergographic operations for AND gate, rather framework in previous schemes. We experimentally demonstrate that our carefulatorial to anoverate florence in time cap to USP), benefits the flow of the province of the contraction is coften if an large cans of pathing schemes we companying all larges in gateful gate, but highers.

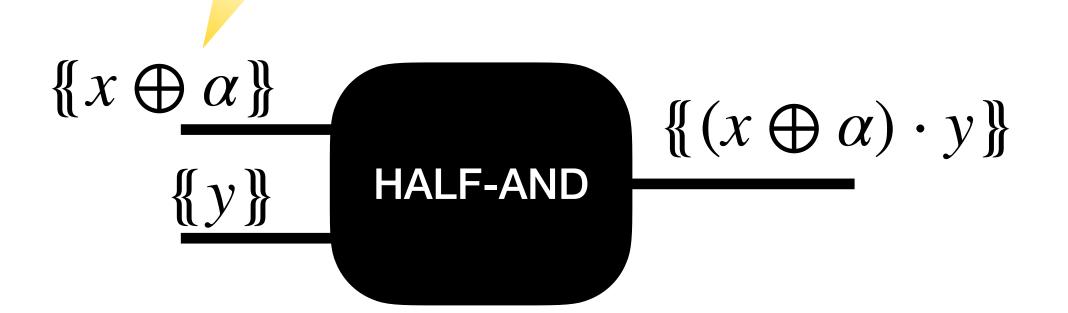
1 Introduction

Yeo's garbled circuit technique remains one of the mess promising and actively studied methods for secuse multi party computation. The first implementation of secuse two-party computation (IPC) [26] used Yao's basic garbled circuit appearsh, and it remains the primary (but not only) paradigm for the many EPC implementation that have been developed over the past ten years [25, 28, 18, 14, 21, 12]. Because the generation and execution of gates benefits from advances in processor speed (in particular, bardware support for cryptographic operations) as well as the increasing availability of large numbers of create, the computation time and cost for garbled circuit protocols has dropped demantically. Thus, the main bot femals for EPC processed in network bandwidth which is performinantly due to the transmission of garbled gates. Many sprintrations in 2PC have bounded on solutions the creates of the garbled circuits themselves [27, 29, 19] and solveing the number of circuits required (in the case of malicines occurity) [24, 29, 22, 15, 8]. Our work reduces the overall sor of garbled circuits by reducing the amount of data text receives to be teamforted for each garbled circuits by reducing the amount of data text receives to be teamforted for each garbled gate.



$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}, \{\!\{x\}\!\}, \{\!\{y\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





$$\Delta \leftarrow \{0,1\}^{\lambda}$$

$$\langle X, X \oplus x \cdot \Delta \rangle = \text{keyPart}(\{\{x \oplus \alpha\}\})$$

 $\langle Y, Y \oplus y \cdot (\Delta, \mu, 1) \rangle = \{\{y\}\}$

Enc(
$$X, Z$$
)
Enc($X \oplus \Delta, Y \oplus Z$)

Garbled Circuit

In 34th Euroceypt, Sofia, Eulgaria, April 2015

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Half Gates

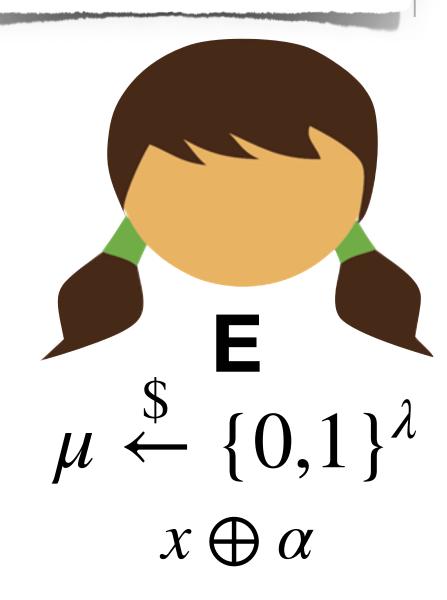
Samee Zahur, Mike Rosulek, and David Eva

University of Virginia (sames, exam) @virginia.

Abstract. The well-harven classical constructions of public circuits we fore eighterteet; per gate, although rations methods have been proposed to reclaim this cost. The best previously known methods for optimizing AND gates (two eighterteet); Profess et al., ASLACRYPT 1000) and XOR gates (two eighterteet); Rotestificous used the best known method compatible with flor-KOR gates (have eighterteet); Rotestificous and the best known method compatible with flor-KOR gates (have eighterteet); Rotestificous and the best known method compatible with flor-KOR gates (have eighterteet); Rotestificous and KOR gates wing aero capherteets, resulting in smaller gathed circuits than any prior scheme. The main little whiched was constructions the band on AND gate into mortally gates and which was constructionally to be and or particular with a single eligibetrica, so our communions uses two eighteens for each AND gate state that the evaluator must perform two expectations operations for each AND gate into mortal scheme. We experimentally demonstrate that our gatemag scheme leads to interestin facetees in time (ap 10 TM). Individual top 2016), and amage use (up to 2016) core coveral benchmark applications. We show that our construction is optimal for a large case of pathing activeness recomposing all learners practical garding beduniques.

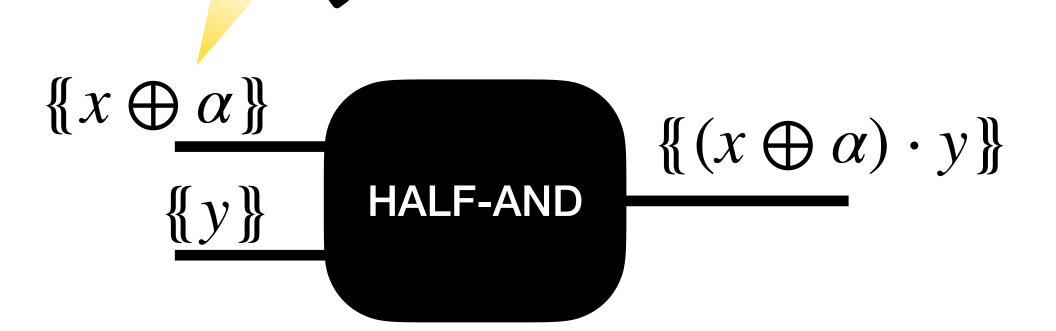
1 Introduction

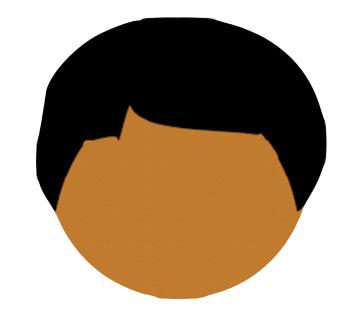
Yor's garbled direati technique transitus one of the mess promising and authorly studied methods for source multi-party computation. The first implementation of source two-party computation (CPC) [26] used Yan's basic garbled circuit approach, and it remains the primary (but not only) paradigm for the many 2PC implementations that have been developed over the past ten years [25, 26, 18, 14, 21, 12]. Because the generation and execution of gaths benefits from advances in processor speed (in particular, hardware suspentivercryytographic operations) as well as the increasing availability of large sumbers of serus, the computation time and cost for garbled circuit protocols has dropped demantically. Thus, the main bottleneck for 2PC protocols is netwerk sundwidth which is predominantly due to the transmission of garbled gases. Many optimizations in 2PC have focused on exclusing the size of the garbled circuits themselves [27, 20, 19] and solveing the number of circuits required [in the case of malicious occurity) [24, 29, 22, 15, a). Our work reduces the overall size of garbled circuits by reducing the amount of data that needs to be transferred for each garbled gate.



$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}, \{\!\{x\}\!\}, \{\!\{y\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





$$\Delta \leftarrow \{0,1\}^{\lambda}$$

$$\langle X, X \oplus (x \oplus \alpha) \cdot \Delta \rangle = \text{keyPart}(\{\{x \oplus \alpha\}\})$$

 $\langle Y, Y \oplus y \cdot (\Delta, \mu, 1) \rangle = \{\{y\}\}$

Enc(
$$X, Z$$
)
Enc($X \oplus \Delta, Y \oplus Z$)

$$\begin{cases} Z & \text{if } x \oplus \alpha = 0 \\ Z \oplus y \cdot (\Delta, \mu, 1) & \text{otherwise} \end{cases}$$

In 34th Euroceypt, Sofia, Eulgaria, April 23:5

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Haif Ga

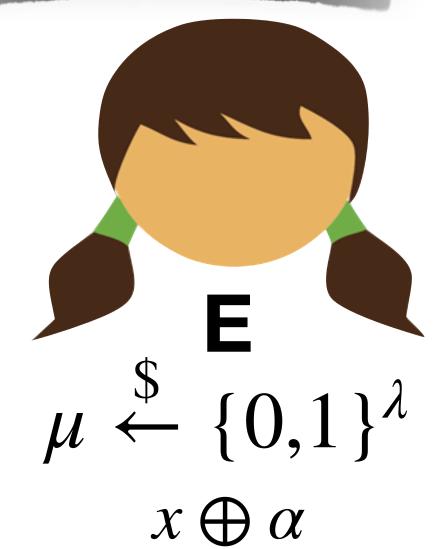
Samee Zahur, Nitte Rosulek, and David Evan

Prigo: Nightbet: vil.com/nargatin University of Virginia (sames, e.a.n.s) @virgi Drogen State University structed region of the control of th

Albeit mit. The well-harwen vissoloid constructions of public viewies use first eightenest; per gate, although entities method; have been supposed foredone this cost. The best gate, although entities method for opinizing AND gates (two eightenests; Perkin et al., ASIACROFT 1000) and XOB gates (two eightenests; Edistrikes and Schneider, ECALF 2003) were incorporable, so meeting-hemotesions used the best known method compatible with first-KOB gates (two eightenests; Rodesmiker and Schneider, ECALF 2003). In this work we show how to simultaneously garble AND pates using two eightenests and KOB gates using two eightenests and KOB gates using two eightenests; resulting in smaller particle circuits than any grice scheme. The main lites belief or sensiting in smaller particle circuits than any grice scheme. The main lites belief or weather in the local first belief or sensiting or compatible with local XCD gates that method gates and be gathed with a single eighternest, so our communities met two eighterness for each AND gate inter that one garpitals with local XCD gates. The pairs for the recording in the list that the evaluator mass perform two exponentative documentate that our sarbing scheme healt to innover all tocease in time top to ETM LiteralWide (op to 2014), and amage use (up to 2014) cover coveral benchmark applications. We show that our construction is outstand for a large caus of patting actiones encomposing all known practical garding techniques.

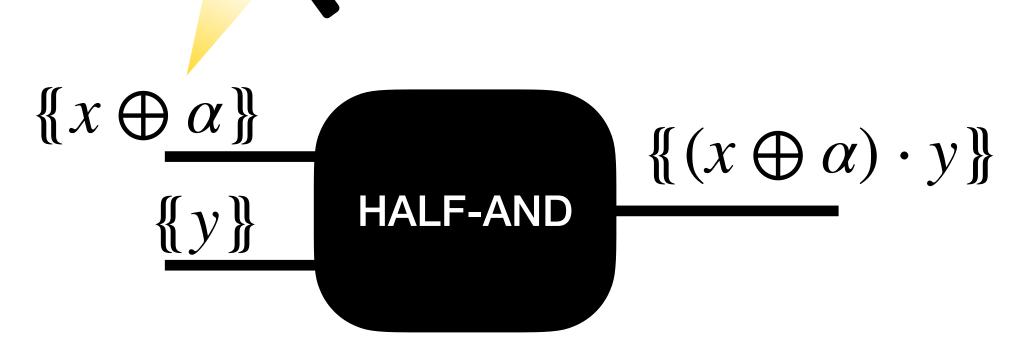
1 Introduction

Yeo's garbled direal: technique remains one of the mess promising and actively memethods for secure multi-party computation. The first implementation of secure tparty computation (JPC) [26] used Yao's basic garbled circuit appearsh, and it remthe primary (but not only) paradigm for the many LPC implementations that have bedeveloped over the part sen years [25, 28, 18, 14, 21, 12]. Because the generation execution of gates benefits from advances in processor speed (in particular, bards supportforceryptographic operation) as well as the interesting reministrity of large as bern of certs, the computation time and cost for garbled circuit protocols has drop demantically. Thus, the main bottleneck for EPC protocols is network bandwidth will be pedominantly due to the turnsmission of garbled gates. Many optimizations in I have become demandating the size of the partled circuits themselves [27, 20, 19], seducing the number of circuits required (in the case of multicious sociality) [24, 29, 13, 18]. Our work reduces the coveral som of garbled circuits by reducing the amountate that models is be togethered for each residuely one.



$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}, \{\!\{x\}\!\}, \{\!\{y\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





$$\Delta \leftarrow \{0,1\}^{\lambda}$$

$$\langle X, X \oplus (x \oplus \alpha) \cdot \Delta \rangle = \text{keyPart}(\{\{x \oplus \alpha\}\})$$

 $\langle Y, Y \oplus y \cdot (\Delta, \mu, 1) \rangle = \{\{y\}\}$

Enc(
$$X$$
, Z)
Enc($X \oplus \Delta$, $Y \oplus Z$)

In 34th Eurocyps, Sofia, Eulgaria, April 2315

Two Halves Make a Whole Reducing Data Transfer in Garbled Circuits using Haif G

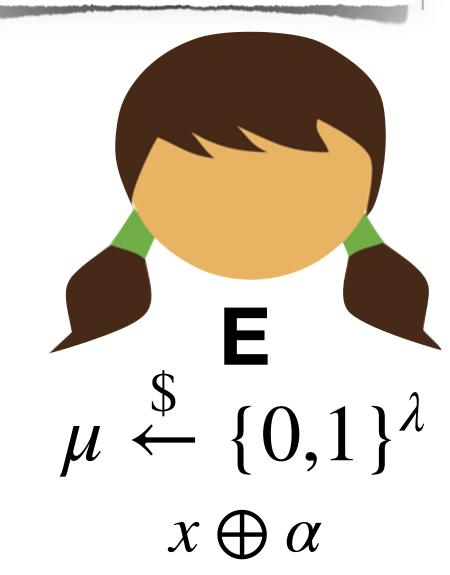
Samee Zahur, Mike Rosulek, and David Eva

Into::MigniseEvil.commangates
University of Virginia (sames,evans)@virginia
Decembrace National Common State Library (sames)

Alternat. The well-brown classical count actions of public circuits use for alphanetts per gate, although surface methods for opinizing AND gates from phenometric Parks et al., ASLACIANT 1000) and XOB gates from alphanette. Parks et al., ASLACIANT 1000) and XOB gates from rightness Kolestikov and Schneidet, EALE 2003) were incorrotation, to meet implementations used the best known method compatible with flow-KOB gates (draw-phenometric Robernatov and Schneider, EALE 2003). In this work we show to to simultaneously gardia AND gates using two eighestests and KOB gates using roc eighestests and KOB gates using two eighestests and KOB gates using two righestests and KOB gates using two righestests and KOB gates with two flows from the published was construction in the total or AND gates for which can garry known one input. Each half-quae cambe gardi with a single dighterest, as our communication was two cipterestes for each AN gate while being compatible with lose XOB gates. The point for the reduction size is that the evaluation rates perform two eraptographic operations or AN gate, rather than one on in previous schemes. We experimentally demonstrate does not retain a strength and samply use (up to 2045) over coveral banchmark application where the other construction is optimal for a large cause of pathing scheme encomposing all acres proclassing of the potentials.

1 Introduction

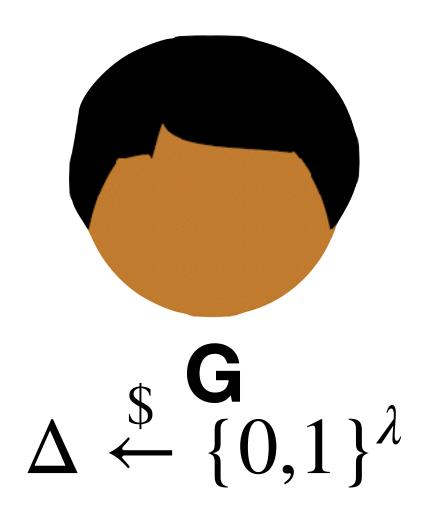
Yao's gurbled circuit sechnique remains one of the mess promiting and archely not methods for necuse multi-party computation. The first implementation of necuse to party computation (PC) [26] used Yao's basic gurbled circuit approach, and it remains primary (but not only) paradigm for the many 2PC implementations that have be developed over the past ten years [25, 20, 10, 14, 21, 12]. Because the generation is execution of gaths bentlies from advances in processor speed (in particular, hards support for cryptographic operation) as well as the increasing reminibility of large as bers of overs, the computation time and cost for garbed circuit protocols has drop dramatically. Thus, the main bottleneck for 2PC protocols is network sandwidth whis predominantly due to the transmission of particul gates. Many optimizations in 2 have boused on soluting the size of the garbed circuits themselves [27, 20, 19] androing the number of circuits required (in the case of maliciness occurity) [24, 29, 15, b.]. Our work reduces the overall size of gathed circuits by reducing the immendate that model to be transferred for each garbled gates.



No opportunity for selective abort

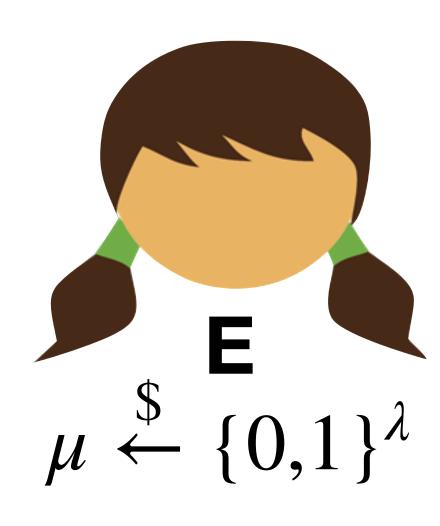
$$\{x\}$$

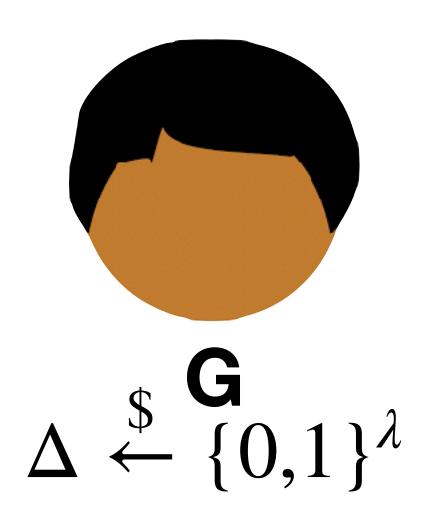
$$\{y\}$$
AND

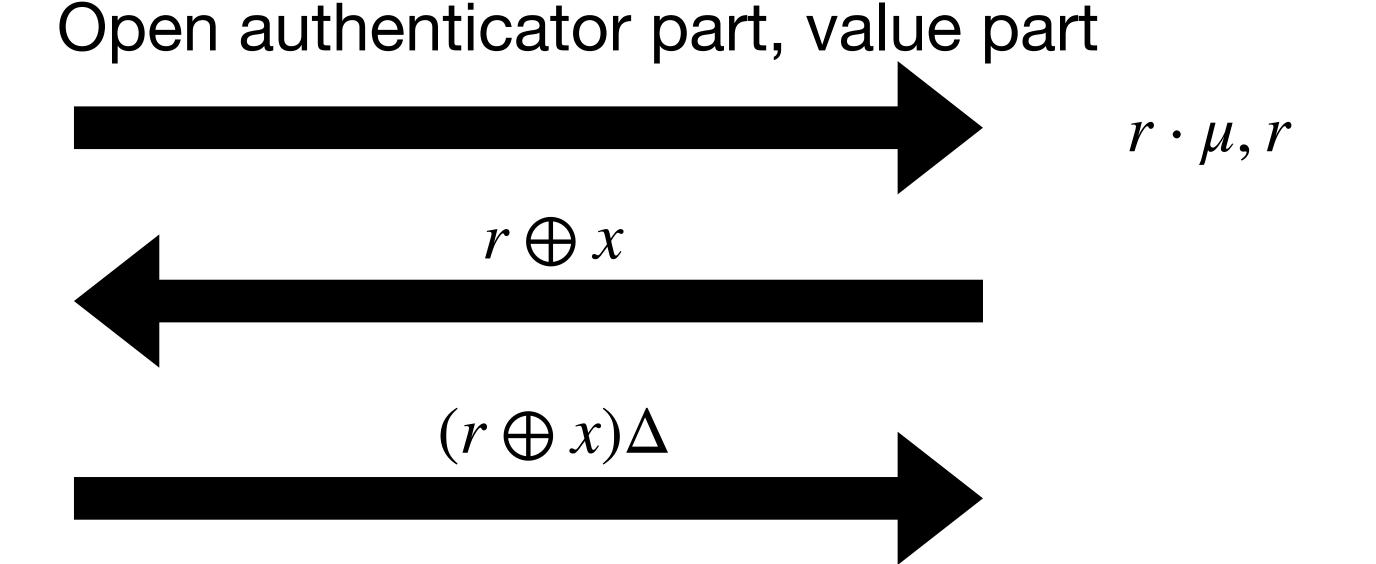


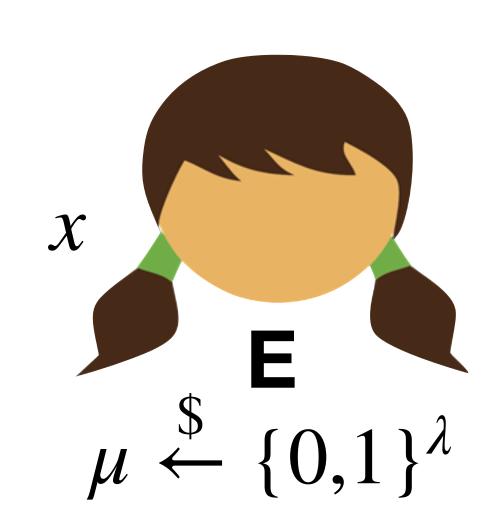
$$\left\{\begin{array}{c} \left\{(x \oplus \alpha) \cdot y\right\} \\ \left\{(y \oplus \beta) \cdot \alpha\right\} \end{array}\right\} \text{ half gates}$$

$$\left\{\begin{array}{c} \left\{(\alpha \cdot \beta)\right\} \\ \left\{(x \cdot y)\right\} \end{array}\right\}$$



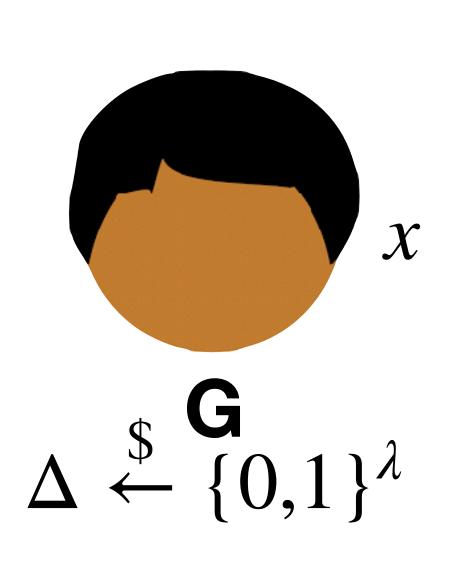






G input wire

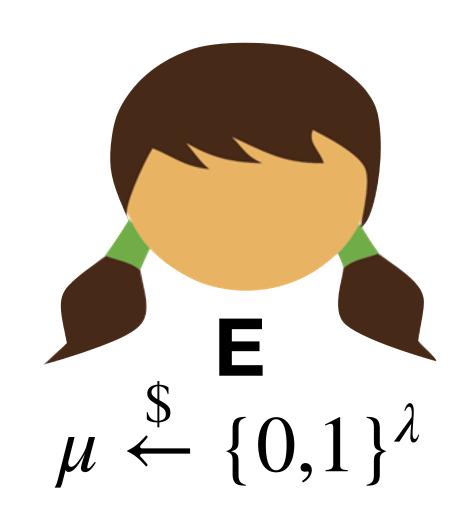
 $r \cdot \Delta, r$

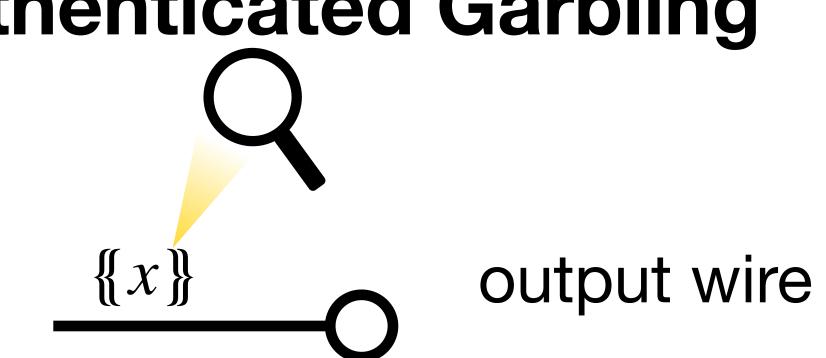


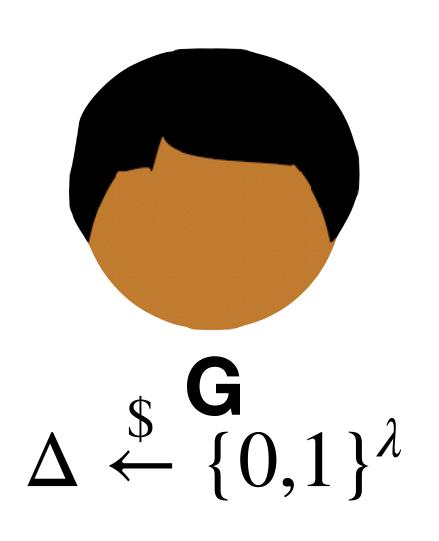
Open key part, value part

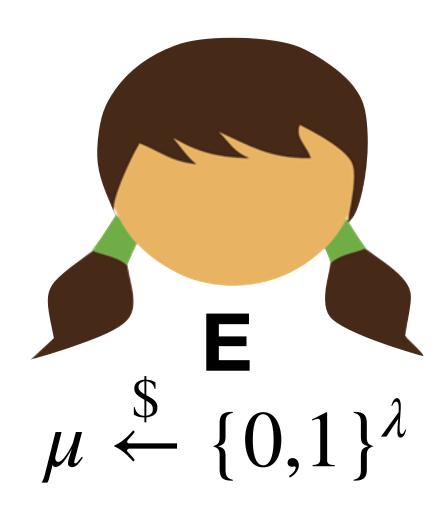
$$r \oplus x$$

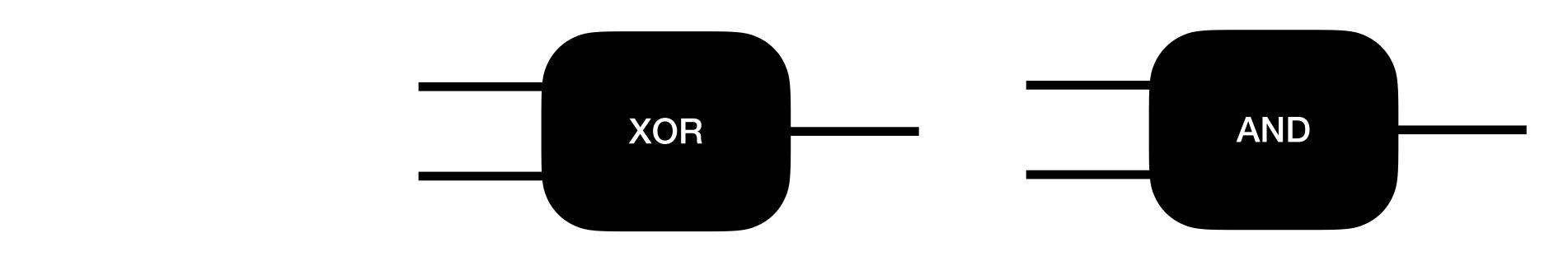
$$\{x\} = [x \cdot \Delta, x \cdot \mu, x]$$

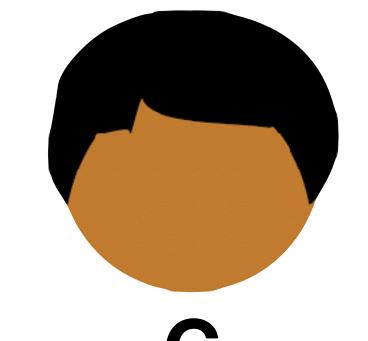








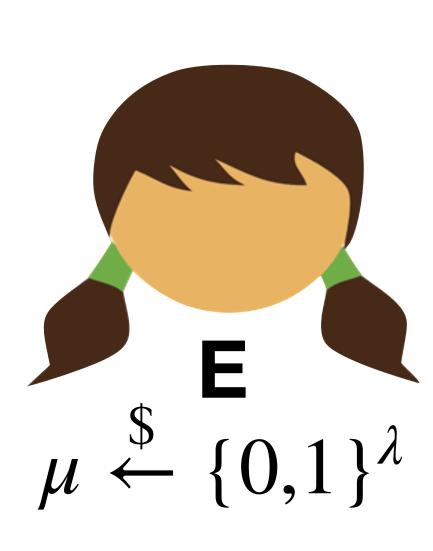




 $\Delta \leftarrow \{0,1\}^{\lambda}$

E input wire

G input wire



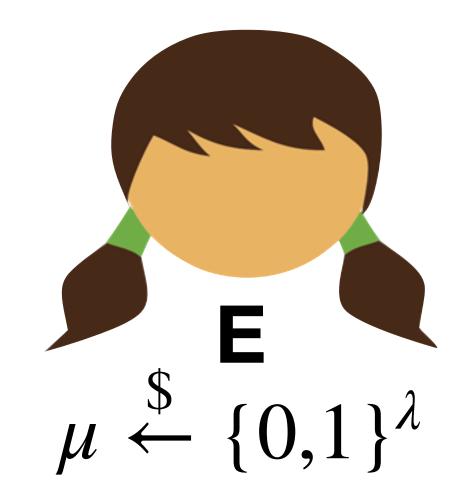
Preprocessing Functionality

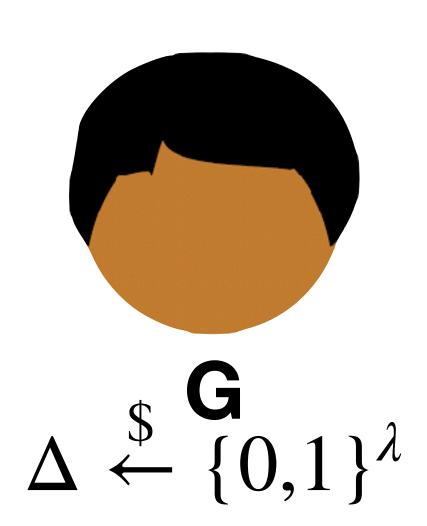
Suppose G and E have access to a doubly authenticated multiplication triple

$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}$$

where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0, 1\}$

Is this an easier problem?





Preprocessing Functionality

Suppose G and E have access to a doubly authenticated multiplication triple

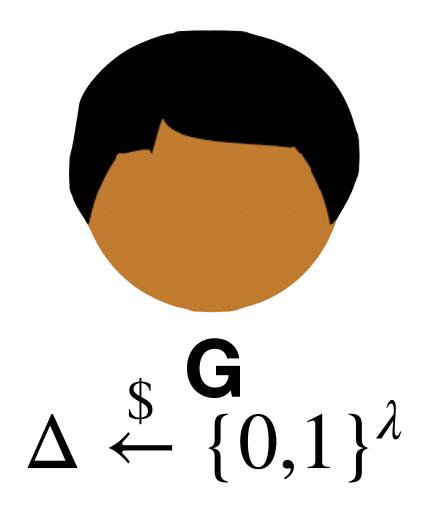
$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}$$

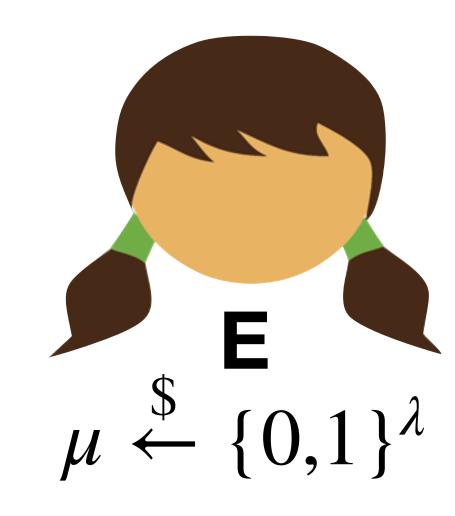
where $\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$





Random bits only; not dependent on inputs Can be computed all at once; no circuit topology





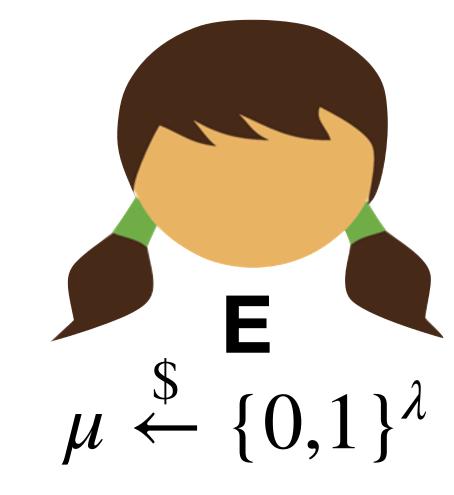
Preprocessing Functionality

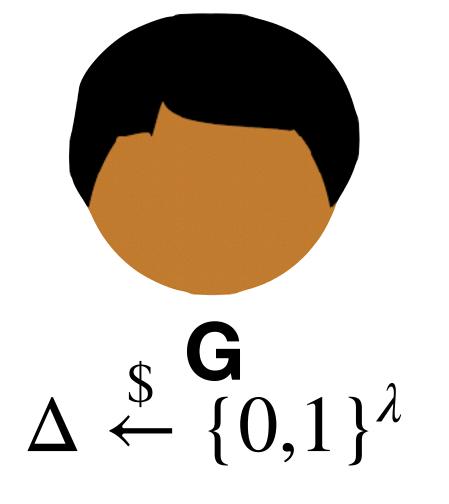
Suppose G and E have access to a doubly authenticated multiplication triple

$$\{\!\{\alpha\}\!\}, \{\!\{\beta\}\!\}, \{\!\{\alpha \cdot \beta\}\!\}$$

where
$$\alpha, \beta \stackrel{\$}{\leftarrow} \{0,1\}$$

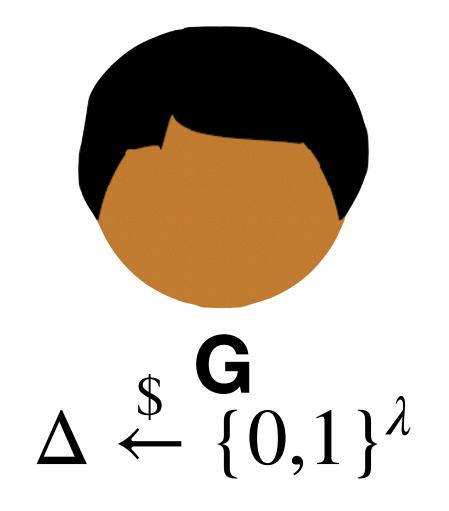
Is this an easier problem?





How do parties implement this?

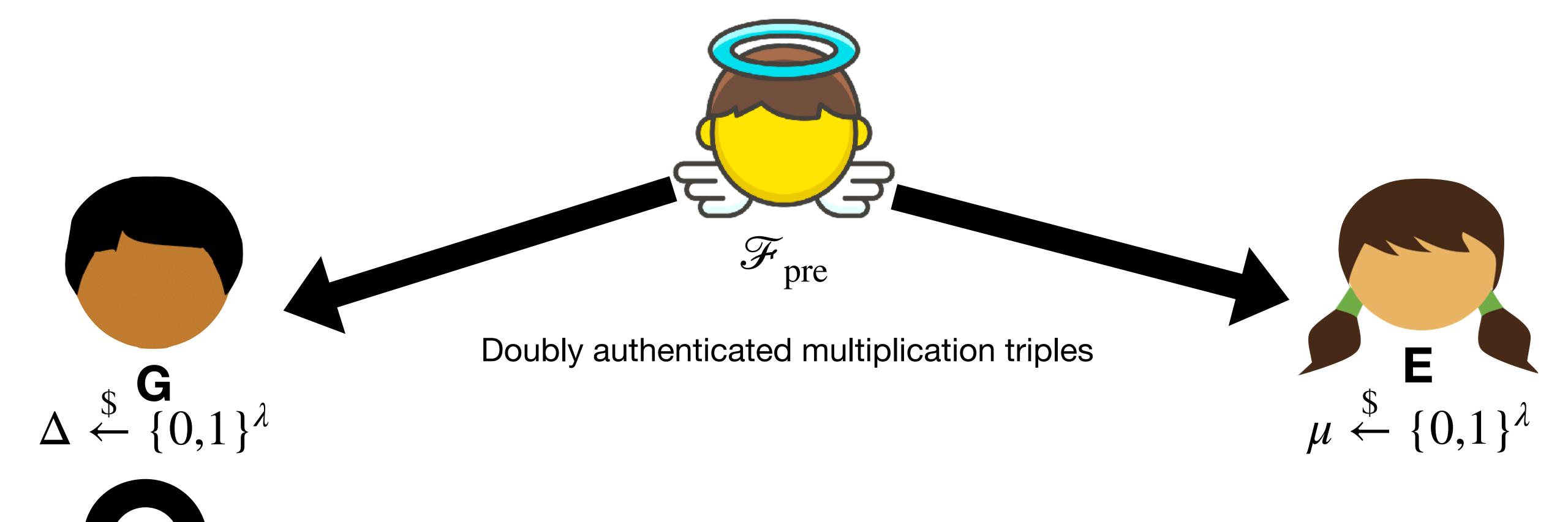
Somewhat complicated, but basically they use cut and choose!



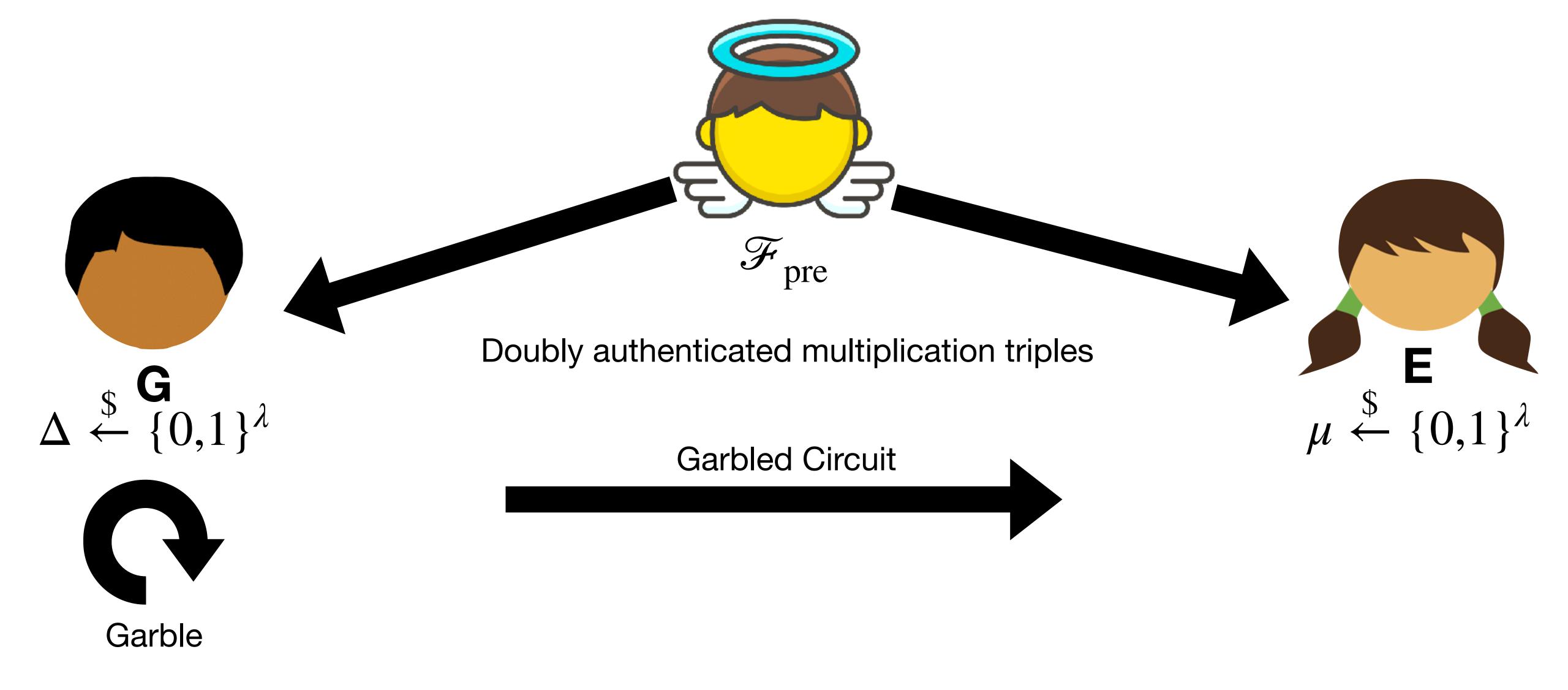


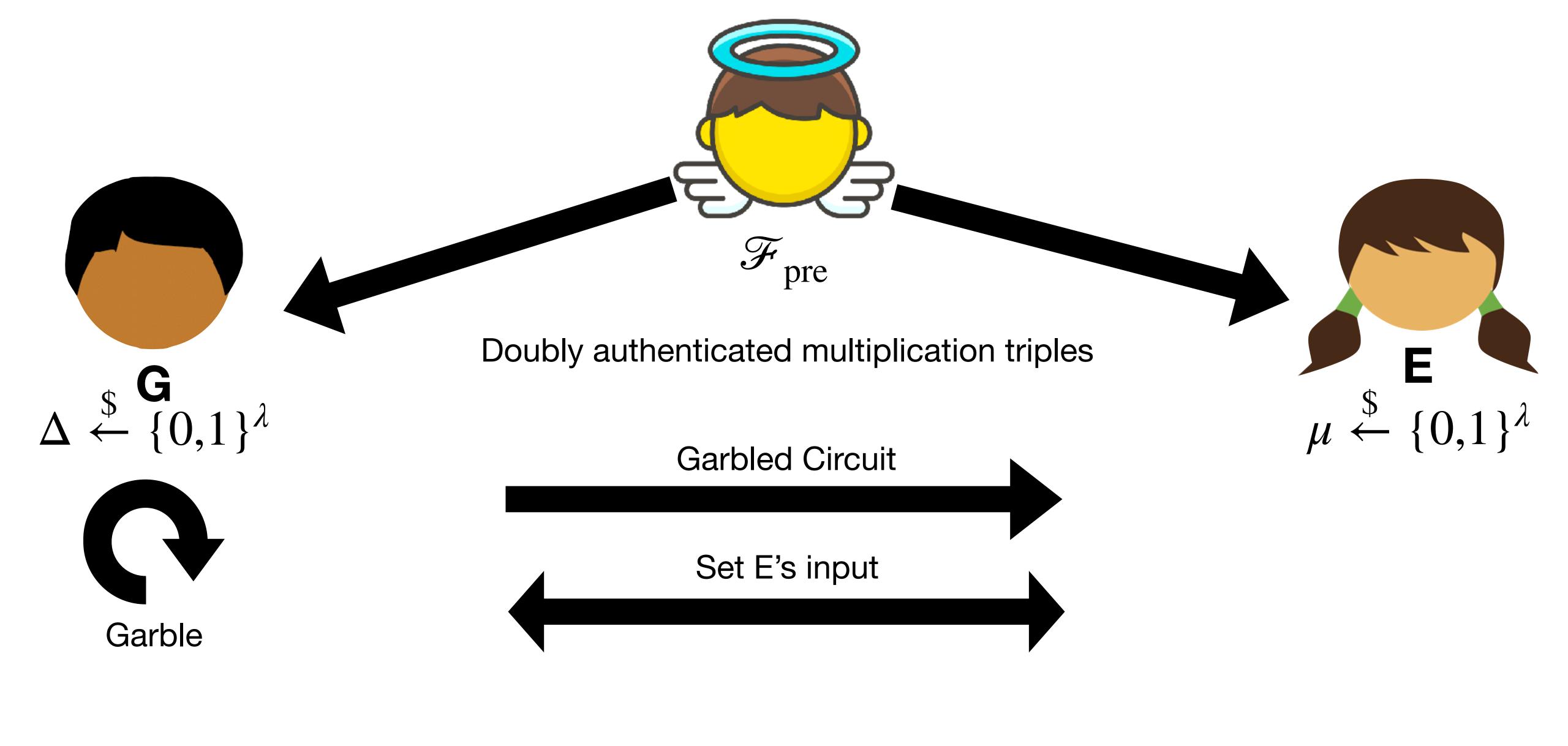


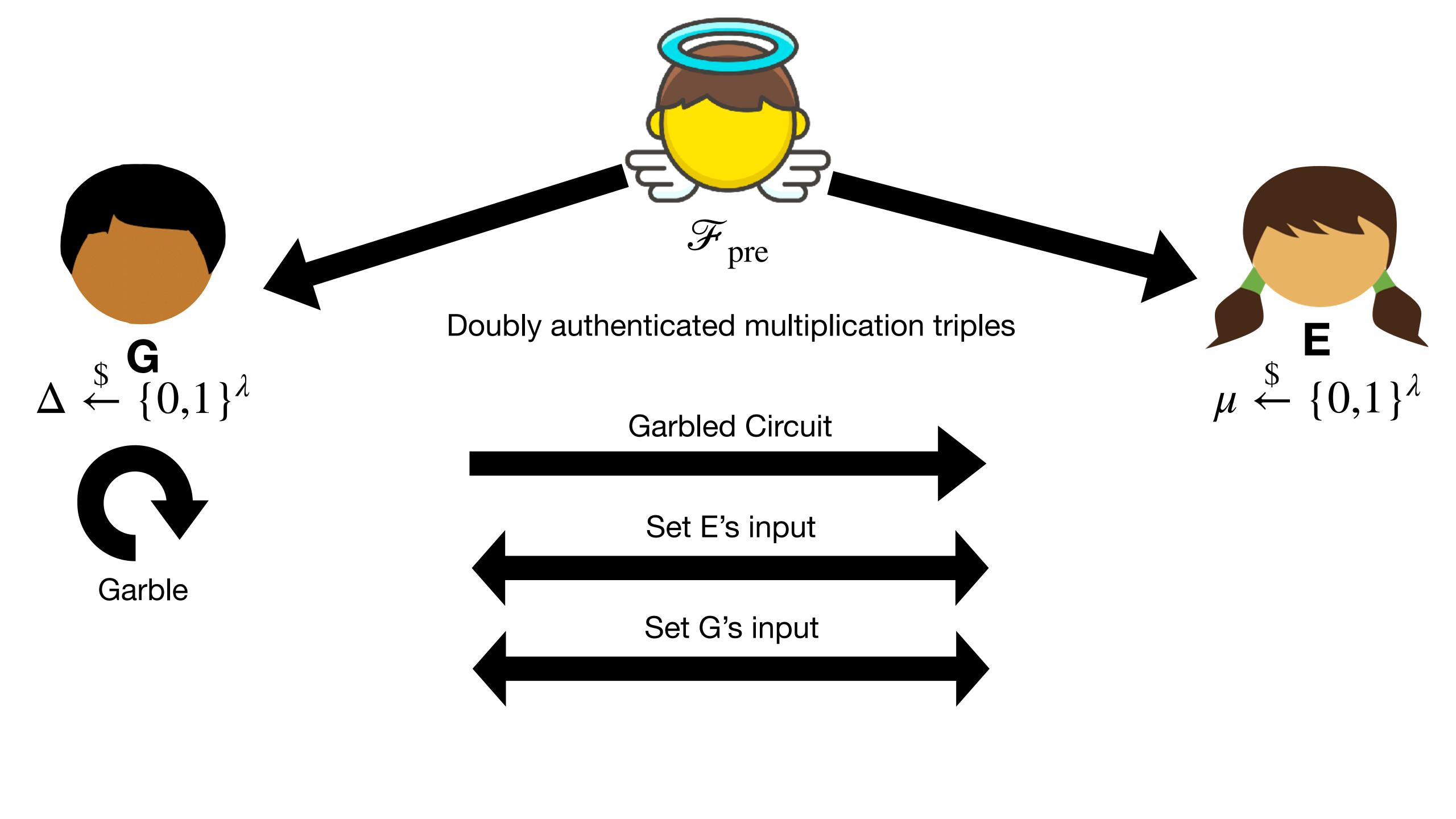
$$\mu \stackrel{\$}{\leftarrow} \{0,1\}^{\lambda}$$

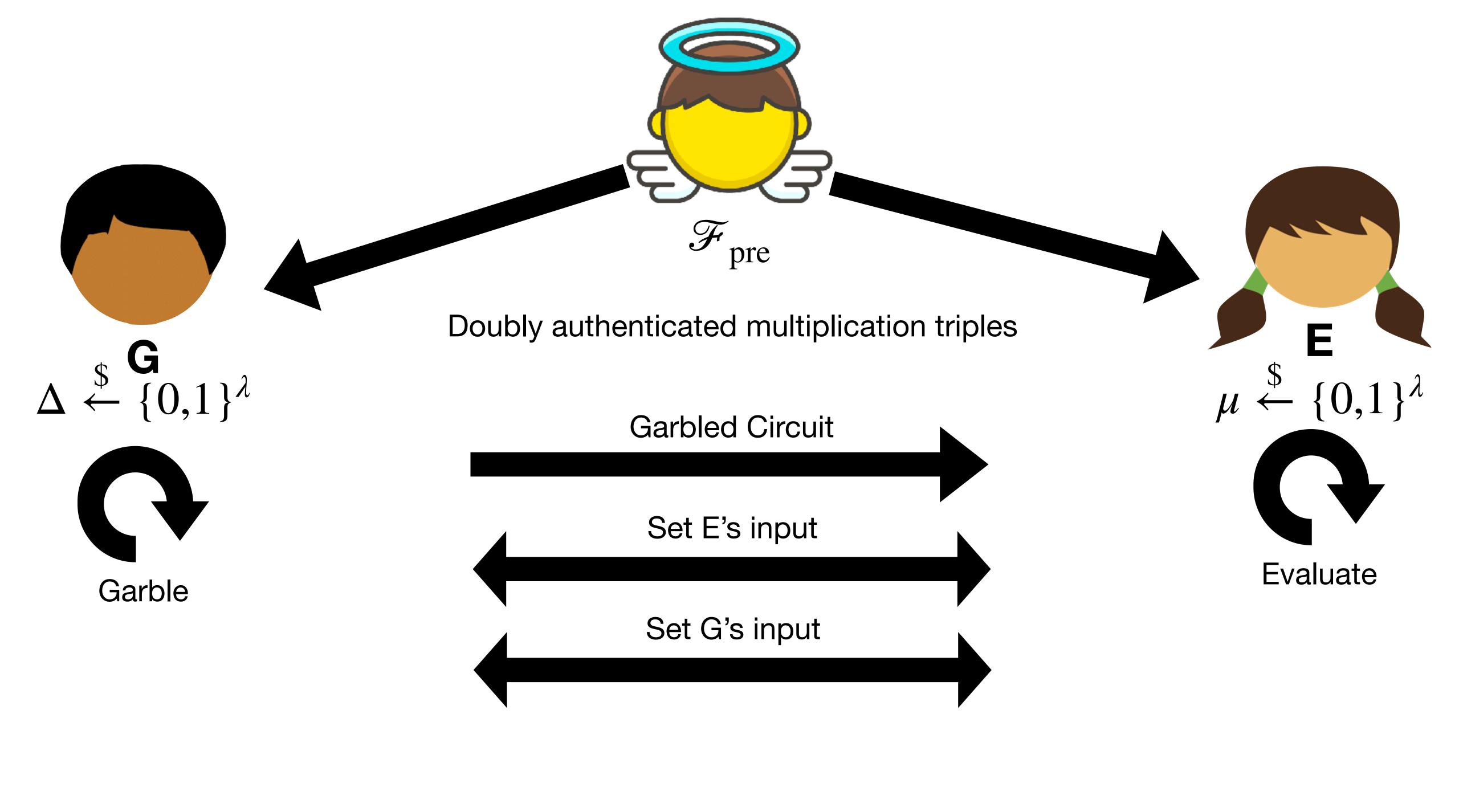


Garble









Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation

Xiao Wang University of Maryland wangxiao@cs.und.edu

Samuel Ranellucci University of Maryland George Mason University Jonathan Katz University of Maryland jkatz@cs.umd.edu

Abstract

samuel@umd.edu

We propose a simple and efficient framework for obtaining efficient constant-round protocols for maliciously secure two-party computation. Our framework uses a function-independent preprocessing phase to generate authenticated information for the two parties; this information is then used to construct a *single* "authenticated" garbled circuit which is transmitted and evaluated.

We also show how to efficiently instantiate the preprocessing phase by designing a highly optimized version of the TinyOT protocol by Nielsen et al. Our overall protocol outperforms existing work in both the single-execution and amortized settings, with or without preprocessing:

- In the single-execution setting, our protocol evaluates an AES circuit with malicious security in 37 ms with an online time of just 1 ms. Previous work with the best online time (also 1 ms) requires 124 ms in total; previous work with the best total time requires 62 ms (with 14 ms online time).
- If we amortize the computation over 1024 executions, each AES computation requires just 6.7 ms
 with roughly the same online time as above. The best previous work in the amortized setting has
 roughly the same total time but does not support function-independent preprocessing.

Our work shows that the performance penalty for maliciously secure two-party computation (as compared to semi-honest security) is much smaller than previously believed.

1 Introduction

Protocols for secure two-party computation (2PC) allow two parties to compute an agreed-upon function of their inputs without revealing anything additional to each other. Although originally viewed as impractical, protocols for generic 2PC in the semi-honest setting based on Yao's garbled-circuit protocol [Yao86] have seen tremendous efficiency improvements over the past several years [MNPS04, HEKM11, ZRE15, KS08, KMR14, ALSZ13, BHKR13, PSSW09].

While these results are impressive, semi-honest security—which assumes that both parties follow the protocol honestly yet may try to learn additional information from the execution—is clearly not sufficient for all applications. This has motivated researchers to construct protocols achieving the stronger notion of malicious security. One popular approach for designing constant-round maliciously secure protocols is to apply the "cut-and-choose" technique [LP07, sS11, sS13, KSS12, LP11, HKE13, Lin13, Bra13, FJN14, AMPR14] to Yao's garbled-circuit protocol. For statistical security $2^{-\rho}$, the best approaches using this paradigm require ρ garbled circuits (which is optimal); the most efficient instantiation of this approach, by Wang et al. [WMK17], securely evaluates an AES circuit in 62 ms.

The cut-and-choose approach incurs significant overhead when large circuits are evaluated precisely because ρ garbled circuits need to be transmitted (typically, $\rho \geq 40$). In order to mitigate this, recent works have explored secure computation in an *amortized* setting where the same function is evaluated multiple times

Constant round protocol secure against malicious adversaries for arbitrary Boolean circuits

Used doubly-authenticated multiplication triples to allow E to check values are well-formed, prevent G from performing selective abort attack

Doubly-authenticated multiplication triples can be efficiently constructed using multiplication triples

Today's objectives

Review IT MACs

Construct maliciously secure garbling