Bitwise Garbling Schemes
A Model with $\frac{3}{2}\lambda$-bit Lower Bound of Ciphertexts

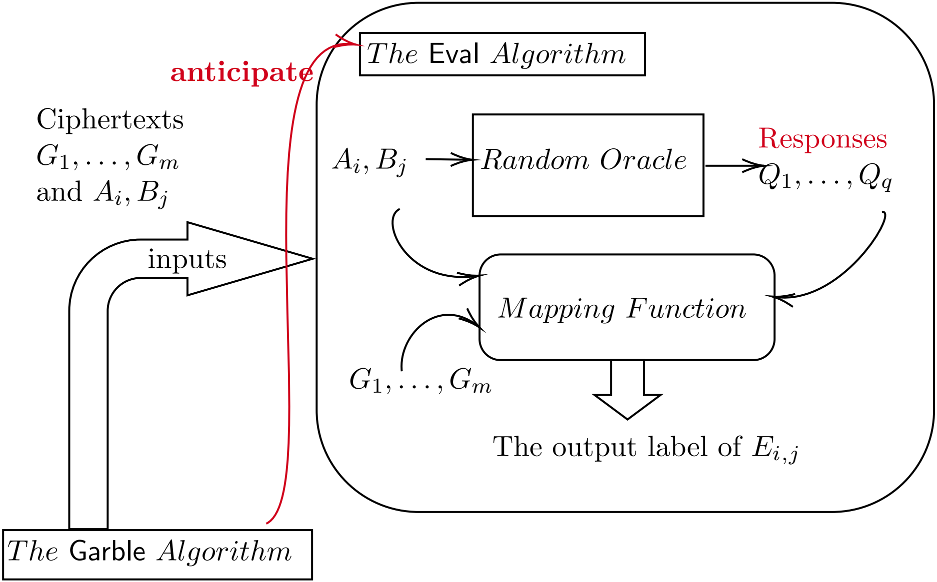
Fei Xu, Honggang Hu and Changhong Xu

Reporter: Fei Xu
2025.8.20

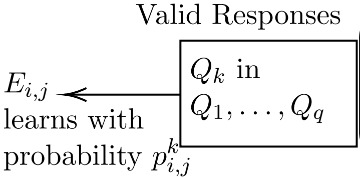
Contributions

- We propose a new model of Bitwise Garbling Schemes, and prove a $\frac{3}{2}\lambda$-bit lower bound of ciphertexts for AND gates with free-XOR. That is to say, the garbling scheme of [RR21] is optimal. When free-XOR is forbidden, we prove a 2λ-bit lower bound of ciphertexts for AND gates.
- We extend our model into garbling of fan-in 3 gates. In this case, we prove a $\frac{7}{4}\lambda$-bit lower bound. This lower bound can only be achieved when the truth table is of even-parity. For example, $a \wedge (b \oplus c)$.

Description of the Model



Valid Responses



We require:

either $p^k_{i,j} = 1$ (Perfect Correctness),
or $|p^k_{i,j} - 1/2| \leq \ poly(\lambda)/2^\lambda$ (Security).

We say oracle response Q_k is **valid** if $p^k_{i,j}$ satisfies one of these two requirements for any $i, j \in \{0, 1\}$.

Classification of Oracle Responses

In our model, we only consider valid responses. For example, no garbling scheme will use half of an input label A_0 to query the random oracle, because $E_{1,0}$ can obtain the response with an advantage $poly(\lambda/2)/2^{\lambda/2}$.

By the way, we can make this invalid response valid by XORing it with a valid response.

Classification of Oracle Responses

n-valid oracle responses

If there is an oracle response Q_k and a set $\mathcal{E}$ of size n, such that $p_k^{(i,j)} = 1$ where $E_{i,j} \in \mathcal{E}$ and $|p_k^{(i,j)} - 1/2| \leq poly(\lambda)/2^\lambda$ where $E_{i,j} \in \{E_{i,j} | i, j \in \{0, 1\}\} \setminus \mathcal{E}$, then Q_k is an n-valid oracle response.

We leave out trivial 0-valid and 4-valid oracle responses. In our model, we only take 2-valid oracle responses into account, since they lead to a better result.

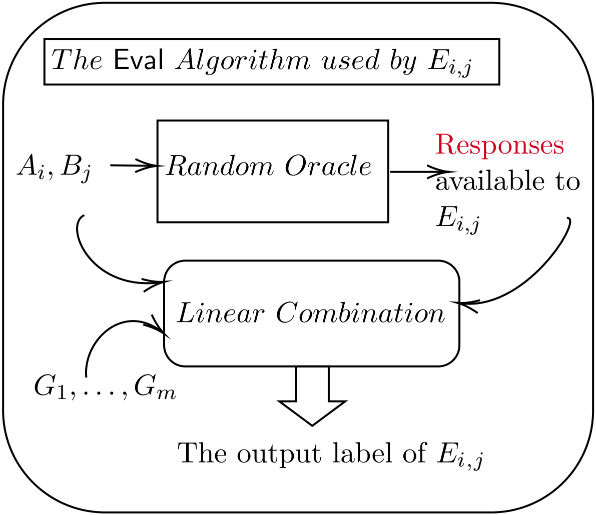
Furthermore, we say that Q_k is associated with the set $\mathcal{E}$. Since $\mathcal{E}$ is of size 2, there are only $\binom{4}{2} = 6$ types of 2-valid oracle responses.

3-Valid Oracle Responses

To see why 3-valid oracle responses do not exist, we assume a 3-valid oracle response Q_k known by $\{E_{0,0}, E_{0,1}, E_{1,0}\}$.
Because $E_{0,0}, E_{0,1}$ obtain Q_k with probability 1, Q_k and B_0 are independent, so we directly assume that $E_{0,0}, E_{0,1}$ use $h(A_0) = Q_k$.
Clearly, $E_{1,0}$ (or $E_{1,1}$) can not obtain valid Q_k with an advantage better than $poly(\lambda)/2^\lambda$.

The work of [JRR25] enhances this conclusion by information theory, and shows that 1-valid responses can be replaced by 2-valid responses through the method of secret sharing.

The Linear Model



Through our classification, $E_{i,j}$ has responses of fixed types. Therefore, we can build a matrix to describe all linear combinations.

Bitwise Linear Garbling Schemes

We follow the idea of linear model in [ZRE15] to propose the model of Bitwise Linear Garbling Schemes, and get the $\frac{3}{2}\lambda$ lower bound of m, which is the length of ciphertexts.

In this model, we require that the mapping function performs linear combinations on its inputs. Since the output labels C_0 and $C_1 = C_0 \oplus \Delta$ must be computed by the same linear combination of responses, we can decide the lower bound of m by studying the rank of a matrix.

Theorem 1

In the model of Bitwise Linear Garbling Schemes, suppose free-XOR is supported. The lower bound of rk is $\frac{5}{2}\lambda$, and therefore $m \geq \frac{3}{2}\lambda$.

However, when we reach the lower bound, we realize that the lower bound of m is equal to the number of responses that an evaluator is unaware of. For example, $E_{0,0}$ does not know all the 1.5λ responses used by $E_{0,1}, E_{1,0}$ and $E_{1,1}$. This inspires a new proof method.

New Proof Method

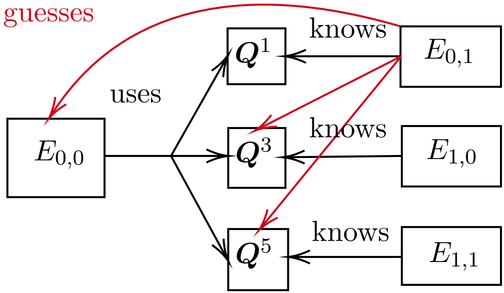
Table 1: 2-valid oracle responses and corresponding sets

	$\boldsymbol{Q}^{i+1}(e.g.\ H(A_i))$	$\boldsymbol{Q}^{i+3}(e.g.\ H(B_i))$	$\boldsymbol{Q}^{i+5}(e.g.\ H(A_0 \oplus B_i))$
$i = 0$	$\{E_{0,0}, E_{0,1}\}$	$\{E_{0,0}, E_{1,0}\}$	$\{E_{0,0}, E_{1,1}\}$
$i = 1$	$\{E_{1,0}, E_{1,1}\}$	$\{E_{0,1}, E_{1,1}\}$	$\{E_{0,1}, E_{1,0}\}$

We include 6 types of 2-valid responses in $\{\boldsymbol{Q}^i | i \in [6]\}$, and suppose that each $\boldsymbol{Q}^i$ is of length n_i.

New Proof Method

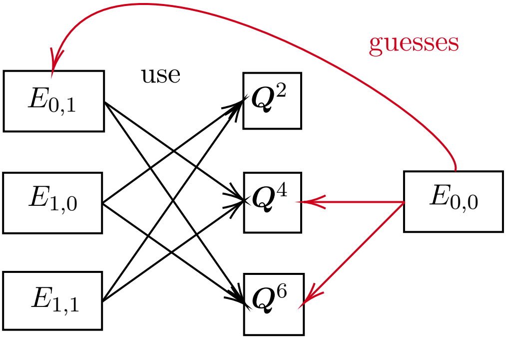
Note that $E_{0,0}$ takes $\boldsymbol{Q}^1, \boldsymbol{Q}^3, \boldsymbol{Q}^5$, input labels and public ciphertexts as the input of the mapping function, while $E_{0,1}$ already learns $\boldsymbol{Q}^1$.



From the view of $E_{0,1}$, learning $\boldsymbol{Q}^3$ and $\boldsymbol{Q}^5$ should not be easier than learning B_0.

Hence, $n_3 + n_5 \geq \lambda$. Similarly, $n_1 + n_5 \geq \lambda$ and $n_1 + n_3 \geq \lambda$.

New Proof Method



From the view of $E_{0,0}$, learning $\boldsymbol{Q}^4$ and $\boldsymbol{Q}^6$ should not be easier than learning B_1.

Hence, $n_4 + n_6 \geq \lambda$.

Similarly, $n_2 + n_6 \geq \lambda$ and $n_2 + n_4 \geq \lambda$. Adding them up, we get $n_2 + n_4 + n_6 \geq 1.5\lambda$.

Lower Bound

In this case, we propose the model of Bitwise Garbling Schemes, which do not restrict the mapping function.

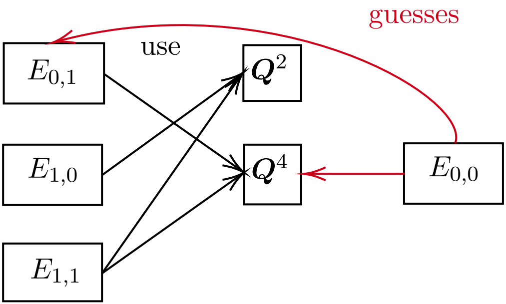
$E_{0,0}$ does not learn 1.5λ responses in $\boldsymbol{Q}^2, \boldsymbol{Q}^4, \boldsymbol{Q}^6$ used by $E_{i,j}$ where $(i, j) \neq (0, 0)$, but they may have the same output label. It is easy to show that ciphertexts of length 1.5λ are needed.

Moreover, the work of [JRR25] indicates how to prove this lower bound by **Shannon Inequalities**.

Without Free-XOR

	$\boldsymbol{Q}^{i+1}(e.g.\ H(A_i))$	$\boldsymbol{Q}^{i+3}(e.g.\ H(B_i))$
$i=0$	$\{E_{0,0}, E_{0,1}\}$	$\{E_{0,0}, E_{1,0}\}$
$i=1$	$\{E_{1,0}, E_{1,1}\}$	$\{E_{0,1}, E_{1,1}\}$

To eliminate free-XOR, we directly assume that $\boldsymbol{Q}^5$ and $\boldsymbol{Q}^6$ do not exist.



Without free-XOR, we require that $n_2 \geq \lambda$ and $n_4 \geq \lambda$.

Lower Bound without Free-XOR

Without free-XOR, we find that $n_i \geq \lambda$ where $i \in [4]$. Since $n_2 + n_4 \geq 2\lambda$, the lower bound of m is 2λ.

Theorem 2

In the model of Bitwise Garbling Schemes, suppose free-XOR is forbidden. Then, $m \geq 2\lambda$.

Extension: Fan-in 3 Garbling

Consider three input labels A_i, B_j, C_k where $i, j, k \in \{0, 1\}$.

n_3-valid oracle responses

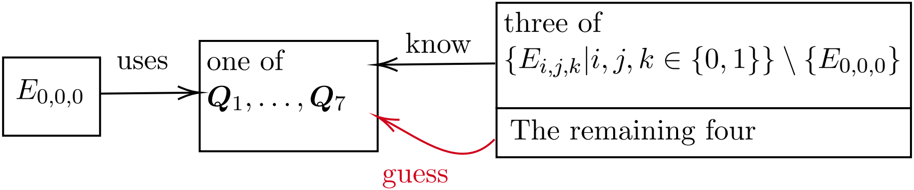
For three input wire labels, if there is an oracle response Q_s and a set $\mathcal{E}$ of size n, such that $p_s^{(i,j,k)} = 1$ where $E_{i,j,k} \in \mathcal{E}$ and $|p_s^{(i,j,k)} - 1/2| \leq poly(\lambda)/2^\lambda$ where $E_{i,j,k} \in \{E_{i,j,k} | i, j, k \in \{0, 1\}\} \setminus \mathcal{E}$, then we say Q_s is an n_3-valid oracle response.

Similar to 2-valid, we can prove that we only need to consider 4_3-valid oracle responses of these representative forms $H(y_1 A_0 \oplus y_2 B_0 \oplus y_3 C_0)$ and $H(y_1 A_0 \oplus y_2 B_0 \oplus y_3 C_0 \oplus \Delta)$ where $(y_1, y_2, y_3) \in \{0, 1\}^3 \setminus \{(0, 0, 0)\}$.

Fan-in 3 Garbling

There are 14 types of 4_3-valid oracle responses $\boldsymbol{Q}_i$ where $i \in [14]$. $E_{0,0,0}$ learns 7 of them, so we assume that these 7 types are in $\{\boldsymbol{Q}_i | i \in [7]\}$. Note that we can refer to the situation with two inputs.

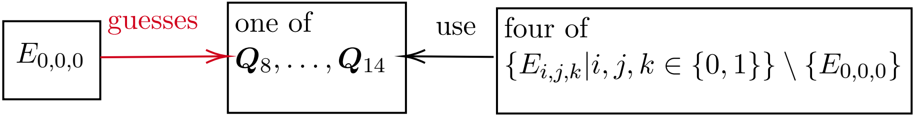
Let $E_{i,j,k}$ guess responses of $E_{0,0,0}$ where $(i,j,k) \neq (0,0,0)$.



There are 7 inequalities for 7 evaluators. Each n_i appears in 4 of 7 inequalities, since 4 of these evaluators do not know $\boldsymbol{Q}_i$. Adding them up, $4\sum_{i=1}^{7} n_i \geq 7\lambda$.

Fan-in 3 Garbling

Let $E_{0,0,0}$ guess responses of $E_{i,j,k}$ where $(i,j,k) \neq (0,0,0)$.



There are also 7 inequalities for 7 evaluators. Each n_i appears in 4 of 7 inequalities, since 4 of them know $\boldsymbol{Q}_i$.

Adding them up, $4\sum_{i=8}^{14} n_i \geq 7\lambda$. Hence, we obtain the 1.75λ-bit lower bound for fan-in 3 garbling.

The Corresponding Construction

We prove the $\frac{7}{4}\lambda$ lower bound of ciphertexts for fan-in 3 garbling. Similar to [RR21], we can obtain the corresponding construction by slicing. However, as we observe in [RR21], the single bit of the entire output label is computed in the form of half-gates garbling scheme. It is easy to check that this construction does not work when the truth table is of odd parity.

Intuitive Extension: Fan-in w Garbling

Let us consider a higher fan-in gate with w pairs of input wire labels $\{W_i, W_i \oplus \Delta | i \in [w]\}$. **Intuitively**, we assume that oracle responses are *indeed* generated by querying the random oracle in the form $H(\bigoplus_{i=1}^{w} y_i W_i)$ or $H(\bigoplus_{i=1}^{w} y_i W_i \oplus \Delta)$ where $y_i \in \{0,1\}$.

- For fan-in 3 garbling, we can prove that choosing these forms is reasonable.
- For fan-in w garbling, we do not find a way to generalize, so this extension is intuitive.

There are $2 \times (2^w - 1)$ types of ${2^{w-1}}_w$-valid oracle responses. We denote all types by $\boldsymbol{Q}_i$ where $i \in [2^{w+1} - 2]$. Suppose $\boldsymbol{Q}_i$ is of length n_i.

Intuitive Extension: Fan-in w Garbling

An evaluator obtains $2^w - 1$ of them, and we assume they are in $\{\boldsymbol{Q}_i | i \in [2^w - 1]\}$. We have $2^w - 1$ inequalities for $2^w - 1$ evaluators. For $2^{w-1}{}_w$-valid oracle responses, each n_i appears in 2^{w-1} of $2^w - 1$ inequalities. Adding them all up,

$$2^{w-1} \sum_{i=1}^{2^w-1} n_i \geq (2^w - 1)\lambda.$$

In the same way, we obtain the

$$\frac{2^w - 1}{2^{w-1}}\lambda = 2\lambda - \frac{1}{2^{w-1}}\lambda$$

lower bound for fan-in w gates. When w increases, the intuitive lower bound of ciphertexts gradually approaches 2λ.

References

ZRE15 Zahur, S., Rosulek, M., Evans, D.: Two halves make a whole - reducing data transfer in garbled circuits using half gates. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 220-250. Springer, Heidelberg (2015).

RR21 Rosulek, M., Roy, L.: Three halves make a whole? Beating the half-gates lower bound for garbled circuits. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part I. LNCS, vol. 12825, pp. 94-124. Springer, Cham (2021).

JRR25 Januzelli, J., Rosulek, M., and Roy L.: Lower bounds for garbled circuits from Shannon-type information inequalities. Cryptology ePrint Archive, Paper 2025/876, 2025.

Thanks for your attention!