Active IC Metering Protocol Security Revisited and Enhanced with Oblivious Transfer

Steffi Roy*, Mohammad Hashemi*§, Fatemeh Ganji*§, Domenic Forte*
University of Florida*, Worcester Polytechnic Institute§
steffiroy@ufl.edu,mhashemi@wpi.edu, fganji@wpi.edu, dforte@ece.ufl.edu

ABSTRACT

Outsourcing semiconductor device fabrication can result in malicious insertions and overbuilding of integrated circuits (ICs) by untrusted foundries without the IP owner's knowledge. Active hardware metering methods attempt to combat IC piracy by requiring fabs to perform an activation protocol with the IP owner for each chip created. In this paper, we have taken a closer look at the IC metering through bus scrambling protocol mentioned in Maes et al., 2009 and we investigate alternatives which employ 1-out of 2 oblivious transfer (OT). Our focus is on Bellare Micali OT and Naor Pinkas OT, which, under certain assumptions, guarantee protection against malicious adversaries. Using OT as an alternative helps with the need to protect the integrity of the private input generated by the chip. Thus, the security of the protocol reduces to the Decisional Diffie Hellman sense. Finally, we discuss possible attacks and show how the proposed protocols could prevent them.

1 INTRODUCTION

Integrated circuits (ICs) have become increasingly complex due to advances in semiconductor fabrication technology where billions of transistors can now be included in a single chip. Many design houses today cannot afford to build and maintain their own IC foundries, so they have to outsource the fabrication to a third party. This horizontal business model relies on collaboration between fabless design houses and foundries, and allows each to concentrate on their strengths. However, this trend has opened the opportunity for adversaries at the fab to steal or misuse the design intellectual property (IP). It is possible for a fab to exceed the agreed upon production volume and sell the excess production in the grey/black market for a high profit. This is known as overbuilding, and can be done by an underground sister company of a renowned manufacturer. In some cases, malicious fabs may attempt to copy a chip's design files through illegal means, such as theft, espionage, or reverse engineering.

The concept of IC metering [9] is a set of protocols that enable the design house to gain post-fabrication control over ICs by passively or actively counting them, analyzing their properties, or remotely disabling them. However, IC metering is only valuable if the correct assumptions and threat models are considered. To address the critical security issues and improve efficiency of the active metering protocols of [9] and [10], Maes et al. [5] proposed improved variants of the bus scrambling-based IC activation protocol. This type of active metering scheme is, in particular, advantageous to FPGAs. For these platforms, instead of producing a hardwired circuit at a foundry, a soft configuration file can be loaded in the field. For this purpose, a non-volatile memory, e.g., flash, often comes with an FPGA to store this configuration file upon powering the FPGA down. Since the configuration file can be read from memory, e.g., by eavesdropping on the configuration bus, FPGA designs are susceptible to cloning. Scrambling of the system bus with a symmetric key is proposed to protect multiple IP modules on an FPGA, which communicate through a common on-chip bus [9]; however, the original schemes were proven insecure in [5].

In this paper, we once again revisit IC metering protocols, but this time we take advantage of advances in oblivious transfer (OT) which strengthens the privacy of the secret bits in the IC metering protocols. As a basis for comparison, we take the state-of-the-art protocol from [5]. We also look at the possible attacks on our protocol and suggest how to address any further security vulnerabilities.

2 BACKGROUND

In this section, we review related terms in cryptography that are necessary to discuss the security of IC metering protocols. We also introduce two Oblivious transfer (OT) protocols, Bellare-Micali OT (BM OT) and Naor-Pinkas OT (NP OT), which form the basis for our proposed IC metering protocols.

2.1 Adversary Model

We consider two adversary models from the field of cryptography. First, the **honest-but-curious** or **semi-honest** adversary is one where the corrupted party or parties merely cooperate to gather information out of the protocol, but do not deviate from its specification. This is a naive adversary model. Protocols in the semi-honest model are quite efficient, and are often an important first step for achieving higher levels of security. The second type are known as **malicious** (so-called active) adversaries that may arbitrarily deviate from the protocol execution and attempt to cheat. The honest-but-curious adversary is often taken into account since it serves as a basis for proving the security even in the presence of a malicious adversary (see Section 4 for a discussion on this).

The proposals for active metering often rely on the following assumptions. The chip needs to be activated right after production, when they are still in possession of the manufacturer; hence, it is plausible to assume that the adversary can effortlessly, and without being caught eavesdrop on communications between the IP owner and the chip. Furthermore, the adversary can alter messages in order to actively attack the protocol. However, the manufacturer is unable to alter the mask set due to the prohibitive costs of producing new masks. More generally, the assumptions usually made in the literature, see, e.g., [9][5][10], are that the attacker does not have full knowledge of the circuit design, and consequently, cannot change the mask or circuit. This assumption reflects the impossibility of easily removing or bypassing the metering mechanism without (eventual) detection.

2.2 Security Assumptions

When discussing security of the protocols mentioned in the next sections, it's important to identify the exact complexity assumptions used by cryptographic protocols.

Let G be any group. In the **Discrete Logarithmic Problem**, let a be an element of G. An integer k that solves the equation $b^k = a$ is termed a discrete logarithm of a to the base b, i.e., $k = \log_b a$. The discrete logarithm problem is considered to be computationally intractable. That is, no efficient classical algorithm is known for computing discrete logarithms in general. In Section 4, we will look at more sophisticated attacks which attempt to break the discrete log problem.

The **Decisional Diffie–Hellman (DDH) assumption** is a computational hardness assumption about a certain problem involving discrete logarithms in cyclic groups. Given some group G of order q and group elements g, where a, b, c are randomly and independently chosen from $\mathbb{Z}_q$, the following two probability distributions are indistinguishable: (g^a, g^b ,g^c) and (g^a, g^b ,g^{ab}).

The **Computational Diffie–Hellman (CDH) assumption** is the assumption that a certain computational problem within a cyclic group is hard. Consider a cyclic group G of order q. The CDH assumption states that, given (g, g^a, g^b) for a randomly-chosen generator g and random $a, b \in \{0, \ldots, q-1\}$, it is computationally intractable to compute the value g^{ab}. Note that the CDH assumption is a weaker assumption than the DDH assumption.

2.3 Oblivious Transfer

Oblivious Transfer (OT) is a two-party protocol between a sender (S) and a receiver (R). The sender S has two secret strings s_0, s_1, and the receiver R has a selection bit $i \in \{0, 1\}$. Upon completion, R learns s_i, but nothing about s_{1-i}, and S learns nothing about i. In other words, S remains oblivious as to what string has been transferred to R. Two OT protocols from the literature that we make use of in our proposed protocols are discussed below.

2.3.1 Bellare-Micali OT (BM OT). Let G be group of prime order p with generator $g \in G$. Let H be a hash function $H : G \longrightarrow \{0, 1\}^l$ (modeled as random oracle). Let h denote a random element of G with $h \neq 1$, and the discrete logarithm of h with respect to g is not known to any party. The sender S inputs are m_0 and m_1 and the receiver R's input is the select bit $s \in \{0, 1\}$ [4]. The protocol works as follows:

(1) The sender S randomly generate C from the generator G: $G \xrightarrow{R} C$, and sends C to the receiver R.
(2) The receiver R chooses random key k such that $\mathbb{Z}_p \xrightarrow{R} k$ and computes two public keys $y_s = g^k$ and $y_{1-s} = h/g^k$ and sends the pair (y_0, y_1) to the sender S.
(3) If $y_0 \cdot y_1 \neq C$ then abort. Otherwise, S encrypts m_0, m_1 with ElGamal using y_0, y_1 respectively, chooses $\mathbb{Z}_p \xrightarrow{R} r_0, r_1$, computes $E_0 = [g^{r_0}, H(y_0^{r_0}) \oplus m_0]$ and $E_1 = [g^{r_1}, H(y_1^{r_1}) \oplus m_1]$, and sends the pair (E_0, E_1) to the R. ElGamal encryption is an asymmetric key encryption algorithm which is based on the Diffie–Hellman key exchange.
(4) R decrypts E_b using k, i.e., $E_b = [V_1, V_2]$, and R computes $m_b = H(v_0^k) \oplus v_1$.

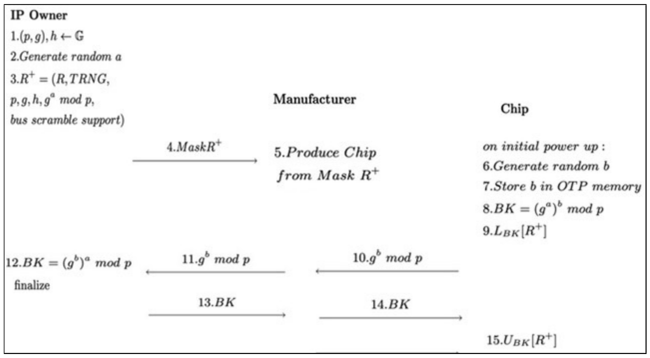

Figure 1: Bus Scrambling with ElGamal key agreement [5]

If R is honest-but-curious, then assuming DDH, R can only decrypt one of E_0 or E_1. If R is malicious, then assuming DDH is not enough; conceivably, R could generate could generate E_0, E_1 in such a way that R knows partial information about their corresponding private keys, and perhaps R can then learn partial information about both m_0, m_1. However, if H is a random oracle, then the protocol is secure under the CDH assumption.

2.3.2 Naor-Pinkas OT (NP OT). Let G be group of prime order q with generator $g \in G$. Similar as above, the sender S inputs are m_0 and m_1 and the receiver R's input is the select bit $s \in \{0, 1\}$ [6]. This protocol works as follows:

(1) R sends the tuple $(g, x = g^a, y = g^b, z_0 = g^{c_0}, z_1 = g^{c_1})$ to S where $a, b, c_{1-s} \in [1, q], c_s = ab \mod q$
(2) S verifies $g^{c_0} \neq g^{c_1}$. It then generates random (r_0, s_0) and (r_1, s_1) and
    (a) Computes $w_0 = x^{s_0} \cdot g^{r_0}$ and encrypts m_0 using the key $z_0^{s_0} \cdot y^{r_0}$.
    (b) Computes $w_1 = x^{s_1} \cdot g^{r_1}$ and encrypts m_1 using the key $z_1^{s_1} \cdot y^{r_1}$. The value w_0, w_1 and the encryption are sent to R
(3) The receiver decrypts using k_s to learn b_s, $k_s = (w_s)^b$

Naor-Pinkas OT is secure against malicious adversaries without random oracles. Its security is based on the DDH assumption alone. Further, R and S computes 5 and 8 exponentiations, respectively. This implies less complexity on the receiver side.

3 ACTIVE-IC METERING PROTOCOL

In this section, we review the bus scrambling IC metering protocol involving ElGamal key agreement proposed in [5]. Then, we further discuss incorporating OT protocols as alternatives to protect the integrity of the private input generated by the chip.

3.1 Bus Scrambling Protocol

The setting for any active IC metering scenario involves communication between these three entities IP owner, foundry and the chip:

- IP Owner: They are the holder of the IP rights on the IC design to be manufactured. IP Owner possesses the design plans of the IC and has mask sets produced from these plans.
- Foundry: Also called as the Manufacturer or fab will manufacture the IC using the mask sets derived from the IP Owner.
- Chip: The manufactured IC, of which we want to meter the production volume.

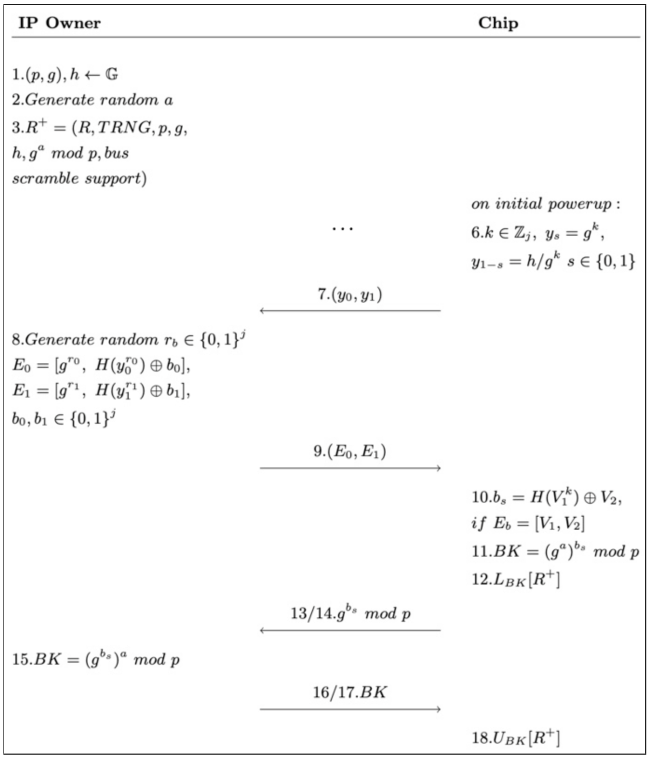
IP Owner
Chip
1.$(p,g), h \leftarrow \mathbb{G}$
2.$Generate\ random\ a$
3.$R^+ = (R, TRNG, p, g,$
$h, g^a\ mod\ p, bus$
$scramble\ support)$
$on\ initial\ powerup:$
…
6.$k \in \mathbb{Z}_j,\ y_s = g^k,$
$y_{1-s} = h/g^k\ s \in \{0,1\}$
7.(y_0, y_1)
8.$Generate\ random\ r_b \in \{0,1\}^j$
$E_0 = [g^{r_0},\ H(y_0^{r_0}) \oplus b_0],$
$E_1 = [g^{r_1},\ H(y_1^{r_1}) \oplus b_1],$
$b_0, b_1 \in \{0,1\}^j$
9.(E_0, E_1)
10.$b_s = H(V_1^k) \oplus V_2,$
$if\ E_b = [V_1, V_2]$
11.$BK = (g^a)^{b_s}\ mod\ p$
12.$L_{BK}[R^+]$
13/14.$g^{b_s}\ mod\ p$
15.$BK = (g^{b_s})^a\ mod\ p$
16/17.BK
18.$U_{BK}[R^+]$

Figure 2: Active IC Metering – with Bellare-Micali OT

We look at this particular Roel Maes et al. protocol [5] involving bus scrambling key and ElGamal encryption that is shown in Figure 1. In this protocol,

- G represents the generation of parameters that are appropriate in order to create a Diffie-Hellman key agreement. The prime p and the generator g of $\mathbb{Z}_p$. R and R^+ are RTL-level descriptions of the original and the enriched (locked) design respectively. IP Owner chooses a random secret a for the key agreement protocol.
- Next, the enriched design is sent for fabrication. On initial power up, the Chip at the foundry generates random b which is stored on the OTP memory and should be kept secret.
- After exchanging $g^a modp$ and $g^b modp$, the IP owner and chip compute a shared key: $(g^a)^b modp = (g^b)^a modp$.
- Afterwards, the IC performs bus scrambling key generation and locks the circuit using the bus scrambling key BK, The bus scrambling key is derived from the shared Diffie-Hellman key using function f: $BK = f[(g^a)^b modp]$.
- $L_{BK}[R^+], U_{BK}[R^+]$ is the bus scrambling based IC-locking mechanism as described in [9]. In contrast to the EPIC scheme, $L_{BK}[R^+]$ does not create a new RTL description. The lock mechanism tells a certain IP module to scramble its bus interface with the key BK, whereas the corresponding $U_{BK}[R^+]$ operation gives the unscrambling key to the other IP modules.

3.1.1 Security Analysis. The security of the scheme relies on the integrity of the IP owner's public exponential a and the private input b generated by the chip. b is generated directly on chip and stored in the memory, where it is vulnerable to theft and fault injection attacks. Fault injection is an active attack that can bypass secure boot mechanisms, extract a secret key, disrupt a program counter, and extract firmware or to manipulate any other secure asset inside an IC (the asset is b in the case of this protocol). A fault can be injected in a variety of ways, such as voltage glitching, clock glitching, laser injection, electromagnetic (EM) injection, etc. A glitch that is analyzed and targeted with precision can create a potential security threat, but it may break the device [2].

Table 1: OT Comparison.

OT	Exponentiation at Sender/IP Owner	Exponentiation at Reciever/Chip	OT's/second	Assumption for Malicious Case
BM OT	4	2	≈ 1041	DDH and CDH
NP OT	8	5	≈ 56	DDH

3.2 Active IC Metering Protocols with OT

When taking a close look at the protocol presented in Figure 1, some similarities between that and the construction suggested by Bellare Micali OT in Section 2.3.1 can be seen. To elaborate on this, suppose that g denotes a generator of a cyclic group G of order p, where p is a large prime. Here, g^x implicitly means $g^x modp$. Let h denote a random element of G with $h \neq 1$, and the discrete logarithm of h with respect to g is not known to any party. At the first stage, the receiver picks a random value $k \in \mathbb{Z}_p$ and computes $y_s = g^k$ and $y_{1-s} = h/g^k$ with s being the select bit, $s \in 0, 1$. Here, the receiver and sender represent the chip and the IP owner, respectively.

Similarly, Naor Pinkas discussed in Section 2.3.2 can be substituted for Bellare Micali OT. For Naor Pinkas OT based IC metering protocol, security depends on indistinguishability of c_s and c_{1-s} which can be tampered by the foundry, to get knowledge about both message bits. As shown in Table 1, the number of exponentiations for NP OT is comparatively more resulting in lesser OT's/ second when considering a standard CPU operating around 2.5 GHz and a very efficient implementation of modular exponentiation for this calculation.

Figure 2 shows Bellare-Micali OT added to the bus scrambling IP metering protocol. Figure 3 shows Naor-Pinkas OT added to the bus scrambling protocol.

3.2.1 Security Advantages of OT-based IP Metering. Here IP owner has the autonomy to generate the value b and OT is used to send this to chip without saving this value in OTP Memory. This can be applied to other active IC metering protocols where an important variable is being generated and stored by the foundry/chip. As discussed in the previous subsection, an attacker can exploit b. Using our method, however, one cannot tamper with evaluation of b by using fault injection or making it a trivial value (e.g., all 1's).

Our protocol also guarantees security against malicious adversaries. The possible active attacks include man-in-the-middle attack (MITM) where the adversary can communicate in the 10th step with both IP owner and Chip to learn the secret. To avoid this, IP owner can evaluate BK with both b_0, b_1 and check for a match.

4 ATTACKS ON THE PROTOCOLS

Generally, the discrete logarithm problem, the fundamental security assumption of OT protocols introduced here, is thought to be intractable in polynomial-time. Nevertheless, under specific scenarios, it is possible to compute it efficiently. Consequently, attacks have been introduced that leverage the weak structure of the cyclic

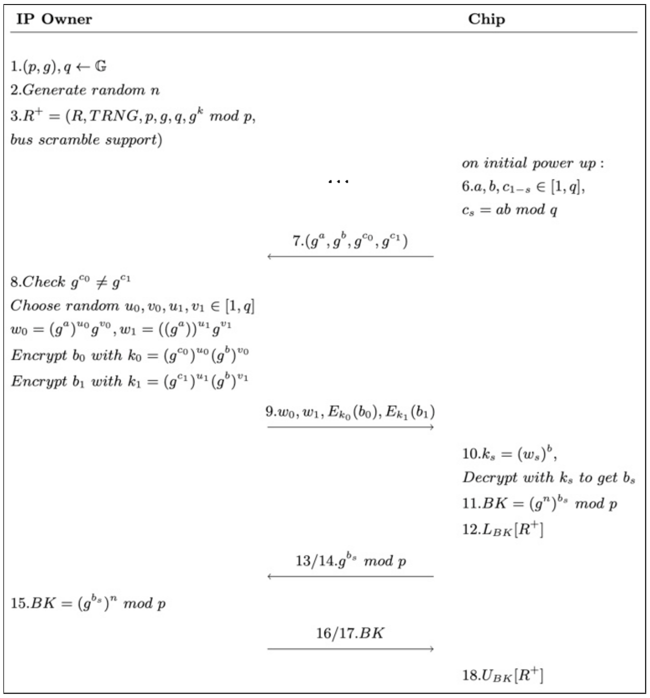
IP Owner
Chip
$1.(p,g),q \leftarrow \mathbb{G}$
$2.Generate\ random\ n$
$3.R^{+} = (R, TRNG, p, g, q, g^{k}\ mod\ p,$
$bus\ scramble\ support)$
$on\ initial\ power\ up:$
$\dots$
$6.a, b, c_{1-s} \in [1,q],$
$c_s = ab\ mod\ q$
$7.(g^{a}, g^{b}, g^{c_0}, g^{c_1})$
$8.Check\ g^{c_0} \neq g^{c_1}$
$Choose\ random\ u_0, v_0, u_1, v_1 \in [1,q]$
$w_0 = (g^{a})^{u_0} g^{v_0}, w_1 = ((g^{a}))^{u_1} g^{v_1}$
$Encrypt\ b_0\ with\ k_0 = (g^{c_0})^{u_0} (g^{b})^{v_0}$
$Encrypt\ b_1\ with\ k_1 = (g^{c_1})^{u_1} (g^{b})^{v_1}$
$9.w_0, w_1, E_{k_0}(b_0), E_{k_1}(b_1)$
$10.k_s = (w_s)^{b},$
$Decrypt\ with\ k_s\ to\ get\ b_s$
$11.BK = (g^{n})^{b_s}\ mod\ p$
$12.L_{BK}[R^{+}]$
$13/14.g^{b_s}\ mod\ p$
$15.BK = (g^{b_s})^{n}\ mod\ p$
$16/17.BK$
$18.U_{BK}[R^{+}]$

Figure 3: Active IC Metering – with Naor-Pinkas OT

group under study. Concretely, the prime number p should be chosen carefully to avoid, e.g., MITM, and Pollard's attack.

MITM Attack: In this type of attack, an adversary can intervene and communicate between IP owner and the chip in steps 11, 13 in Figure 1 and steps 13, 16 in Figures 2 and 3, respectively. This adversary can be the manufacturer itself, though discrete logarithm assumption protects from revealing the secret exponent. The OT-based IC metering gives an extra guarantee that no adversary tampered with the $g^{b} modp$ value through the IP owner check of the value of BK with b_0 and b_1.

The complexity of a brute force attack on the discrete log is O(2^{p}). Suppose p is 1024 bits long, i.e., 300 digits, implying 2^{300} operations. This signifies that it would be difficult for such attacks to succeed. However, there are algorithms which try to break the discrete log faster. For example, "baby-step giant-step" is a form of collision attack which solves discrete logarithm in time O($\sqrt{p}$), Pollard's Rho [8] takes O($\sqrt{p}$), and Index Calculus Algorithm [12] takes sub-exponential time $2^{O(\sqrt{\log p \log\log p})}$. The latter attack does not work on elliptic curve Diffie-Hellman and for Pohlig-Hellman algorithm [7]. Further, the worst-case happens when the input is a group of prime order, with the worst-case time complexity O$\sqrt{p}$. The complexity would also reduce to $O\left(\sum_i e_i(\log n + \sqrt{p_i})\right)$, if $\prod_i p_i^{e_i}$ is the prime factorization of n.

In [1] after one week of pre-computation, it has been shown that it is possible to compute the discrete logarithm in a 512-bit group in one minute by using the number field sieve algorithm. In doing so, the receiver would be able to receive both messages m_0 and m_1 of the Bellare-Micali OT protocol in one minute. To avoid the attack in [1], it is recommended to transition to elliptic curve Diffie-Hellman (ECDH) key exchange with appropriate parameters. This could avoid known feasible cryptanalytic attacks.

Furthermore, there is less chance of these attacks working out if the key size is large. Therefore, NIST [3] gave guidelines on the key strength to avoid attacks in the present where L is the size of the public key, and Diffie-Hellman uses subgroup of $\mathbb{Z}_p^*$ size q, $N = q$ is the size of the private key. Security strength of 112 bits is accepted and L should be larger than 2048 and $N = 224$. As the systems are evolving to run these algorithms faster, one might need to shift to much larger key sizes. Considering post quantum cryptography, this will become important [11].

5 CONCLUSION

We analyzed the cryptograpic activation protocols of IC metering, applying to the bus scrambling protocol with ElGamal encryption by Maes et al. In that protocol, the system bus is scrambled such that the chip is non-functional on start-up and the security relied on the confidentiality of a secret keys stored on the chip. We suggest our OT-based IC metering protocols which are secure against active adversaries and discuss their advantages over the previous protocol. We examine the attacks possible on our protocols and suggest how to practically avoid any security vulnerabilities.

6 ACKNOWLEDGEMENTS

This work was supported by the National Science Foundation under Grant No. 1651701 and the Semiconductor Research Corporation under Task IDs 2991.001 and 2992.001.

REFERENCES

[1] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, et al. 2015. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 5–17.

[2] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. 2012. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proc. IEEE* 100, 11 (2012), 3056–3076.

[3] Elaine Barker and Quynh Dang. 2016. Nist special publication 800-57 part 1, revision 4. *NIST, Tech. Rep* 16 (2016).

[4] Mihir Bellare and Silvio Micali. 1989. Non-interactive oblivious transfer and applications. In *Conference on the Theory and Application of Cryptology*. Springer, 547–557.

[5] Roel Maes, Dries Schellekens, Pim Tuyls, and Ingrid Verbauwhede. 2009. Analysis and design of active IC metering schemes. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 74–81.

[6] Moni Naor and Benny Pinkas. 2001. Efficient oblivious transfer protocols. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*. 448–457.

[7] Stephen Pohlig and Martin Hellman. 1978. An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (corresp.). *IEEE Transactions on information Theory* 24, 1 (1978), 106–110.

[8] J Pollard. 1975. Monte Carlo methods for index computation. *Math. Comp.* 32, 143 (1975).

[9] Jarrod A Roy, Farinaz Koushanfar, and Igor L Markov. 2008. Protecting bus-based hardware IP by secret sharing. In *2008 45th ACM/IEEE Design Automation Conference*. IEEE, 846–851.

[10] Jarrod A Roy, Farinaz Koushanfar, and Igor L Markov. 2010. Ending piracy of integrated circuits. *Computer* 43, 10 (2010), 30–38.

[11] Manuel B Santos, Armando N Pinto, and Paulo Mateus. 2021. Quantum and classical oblivious transfer: A comparative analysis. *IET Quantum Communication* 2, 2 (2021), 42–53.

[12] Oliver Schirokauer, Damian Weber, and Thomas Denny. 1996. Discrete logarithms: the effectiveness of the index calculus method. In *International Algorithmic Number Theory Symposium*. Springer, 337–361.