Cheat-Penalised Quantum Weak Coin-Flipping

Atul Singh Arora, Carl Miller, Mauro E.S. Morales, Jamie Sikora EXTENDED ABSTRACT

Can two parties who are communicating at a distance carry out a coin-flip in such a way that both are assured that the coin-flip was fair? In other words, can two parties who do not trust one another generate a fair random bit without relying on a third party? With classical technology, this task is impossible in the unconditional setting, although it becomes possible if computational hardness assumptions are made (e.g., [MNS09]). In the quantum setting, however, there are secure protocols for coin-flipping that do not make computational hardness assumptions and rely only on minimal physical assumptions [ATSVY00, SR01, SR02, Amb04, Moc04, Moc05, Moc07]. Coin-flipping is a prime example of the unique capabilities of quantum technology for cryptographic tasks, and it was one of the original problems that started the field of quantum cryptography [BB84].

The body of work in two-party cryptography offers many results that are beautiful from a theoretical standpoint but daunting from an experimental standpoint. Secure two-party computation, bit commitment, oblivious transfer, and strong coin-flipping have all been proved to be impossible to perform [Lo97, LC98, ABDR04, LC97, May97]—the best that one can achieve for those tasks are protocols with partial security. In 2007, Mochon [Moc07] offered a ray of hope by proving that *weak* coin-flipping—coin-flipping in which the desired outcome for each party is known—is possible with security bounds arbitrarily close to the ideal security setting, i.e. zero "bias". In particular, he gave families of protocols approaching bias $\epsilon_{\text{Moch}}(k) := 1/(4k+2)$ for each $k > 1$.

However, Mochon's constructions were rather involved and complex. Specifically, the number of rounds of communication grew exponentially as one approached zero bias. While several works have subsequently improved on and enriched Mochon's work [ACG+14, CGS, CK17, Gan17, ARW19], this issue persists. In 2020, Miller [Mil20] proved that any near-perfectly-secure protocol for weak coin-flipping must use an exponential number of communication rounds. Consequently, there is no efficient quantum protocol for the original weak coin-flipping problem. As for space complexity—the number of qubits needed—Mochon's Dip-Dip-Boom protocol ($k = 1$ in the family above) achieves bias $\epsilon_{\text{Moch}}(1) = 1/6$ only uses two qutrits and a qubit. It is not known, for instance, whether a protocol with comparable space complexity exists that goes below bias $\epsilon_{\text{Moch}}(2) = 1/10$.

Cheat-penalised coin-flipping. One way to circumvent Miller's impossibility result is to change the mathematical model on which the proof is based. In particular, the shape of the problem changes significantly if we (following [ABDR04]) introduce a cheat penalty parameter $\Lambda \geq 0$. Suppose that we allow for three possible outputs from Alice and from Bob, denoted 0, 1, and $\perp$, where the outcome $\perp$ indicates that cheating has been detected by the other party. In this case, the cheating party loses Λ coins. Therefore, if Alice wins, she gains 1 point (Bob gains nothing), if Bob wins he gains 1 point (Alice gains nothing), and if either party is caught cheating, they lose Λ points. This protocol, which we call a *Λ-penalty weak coin-flipping protocol*, or **Λ-penWCF** for short, makes a distinction between a party honestly losing the exchange (and receiving a score of 0) and a party getting caught cheating (and receiving a score of $-\Lambda$). This primitive is natural when considered as part of a broader scheme where parties engage in multiple interactions, introducing disincentive for malicious behaviour.

There are a few key differences between the previously-studied version of weak coin-flipping and the cheat-penalised setting. Specifically, in the cheat-penalised setting, each party wishes to maximize their respective *expected reward*, not just the probability that they will win. Thus, we want protocols where neither Alice nor Bob can cheat and obtain an expected reward more than $1/2 + \epsilon$, for a preferably small value of $\epsilon > 0$. In this work, we not only want ϵ, referred to as the **bias**, to be small, but also the round complexity, denoted rc, and the space complexity, denoted sc. This motivates the following questions.

> *To what extent can introducing a cheat penalty improve the efficiency of weak coin-flipping protocols? How large must the cheat penalty be to achieve this?*

Point Games. Kitaev and Mochon [Moc07] introduced various so-called *point games* to design and analyse coin-flipping protocols. Here, we focus on two variants: *time-independent point games*, **TIPG**, and *time-dependent point games*, **TDPG**. A TIPG is specified by two bivariate functions (h, v) where each encodes a finite set of weighted configurations of points on a two-dimensional plane. We use the notation $p[\![x, y]\!]$ to indicate the point (x, y) has weight p where $p \in \mathbb{R}$. A bit more formally, $[\![x, y]\!]$ is bivariate function that is zero everywhere except on input

(x, y) where it evaluates to one. A TIPG (h, v) for (non-penalised) weak coin-flipping must satisfy

$$h + v = \underbrace{\left[\!\left[\frac{1}{2} + \epsilon, \frac{1}{2} + \epsilon\right]\!\right]}_{\text{final config.}} - \underbrace{\left(\frac{1}{2}[\![0, 1]\!] + \frac{1}{2}[\![1, 0]\!]\right)}_{\text{initial config.}} \tag{1}$$

together with extra "validity conditions" that we are suppressing for brevity. For any such TIPG, there exist weak coin-flipping protocols that approach bias ϵ (up to arbitrary precision). As alluded to earlier, Mochon [Moc07] constructed a family of TIPGs parametrised by k that approach bias $\epsilon = 1/4k + 2$, thereby establishing the existence of weak coin-flipping with vanishing bias, $\epsilon \to 0$. However, in 2020, Miller showed that there is a relationship between the round complexity of weak coin-flipping protocols and the norm of h and v in any point game, leading to the conclusion that any weak coin-flipping protocol must have at least $\exp(\Omega(\epsilon^{-1/2}))$ rounds of communication. This renders them necessarily inefficient as $\epsilon \to 0$.

Approximate cheat-penalised TIPGs and how to find them. By revisiting the construction of point games in [Moc07], one can define the notion of a *cheat-penalised TIPG*, **penTIPG**. In essence, here one translates both the "initial" and "final configurations" by Λ (along both axes). While Mochon already informally considered such penTIPGs, his focus was establishing security for weak coin-flipping (without penalty) and not efficiency. Consequently, he did not study such games in further detail. Since here we are concerned with *efficiency* as well, our starting point is finding point games with small norm. It does not take long to realise that a brute force search is hopeless. Our first contribution is a numerical algorithm to find such point games. Not only does our algorithm yield solutions, it does so even for small values of Λ. However, these solutions are *approximate* and we therefore slightly relax the definition of penTIPG as follows.

Definition 1: $(\Lambda, \varepsilon_{\text{approx}})$-penTIPG—Approximate cheat-penalised TIPGs (informal)

We say (h, v) is a $(\Lambda, \varepsilon_{\text{approx}})$-penTIPG with bias ϵ if it satisfies

$$h + v \approx_{\varepsilon_{\text{approx}}} \underbrace{\left[\!\left[\Lambda + \frac{1}{2} + \epsilon, \Lambda + \frac{1}{2} + \epsilon\right]\!\right]}_{\text{final config.}} - \underbrace{\left(\frac{1}{2}[\![\Lambda + 1, \Lambda]\!] + \frac{1}{2}[\![\Lambda, \Lambda + 1]\!]\right)}_{\text{initial config.}} \tag{2}$$

in addition to the "validity conditions" mentioned previously. Here approximation is in terms of the 1-norm. By the *number of points* of (h, v), we mean the number of input pairs that are assigned non-zero weight by h and v, i.e., $|\text{supp}\{h, v\}|$. By the *norm of* (h, v) we mean $\max\{\|h\|_1, \|v\|_1\}$.

We obtain various solutions but we highlight the one that results in a cheat-penalised WCF protocol with final bias $\epsilon = 10^{-8}$, where the cheat penalty is $\Lambda = 0.01$. As for efficiency, it uses 24 qubits and has round complexity more than *three orders of magnitude* lower compared to Miller's lower bound for the analogous WCF protocol, giving a separation between the two settings.

Theorem 1: Existence of approximate cheat-penalised point games with small norm (informal)

We give a numerical algorithm for finding good penTIPGs which, specifically, yields a $(\Lambda, \varepsilon_{\text{approx}})$-penTIPG with bias $\epsilon = 10^{-10}$, norm 1.05 using at most 64 points, for $\Lambda = 0.01$ and $\varepsilon_{\text{approx}} = 10^{-18}$.

The code, together with other penTIPG solutions, are on GitHub [AMMS25]. It is important to emphasise that this result, on its own, does not resolve the central question of achieving efficient and secure weak coin-flipping. Tackling the reduction from point games to protocols in this new regime turns out to be subtle and requires new ideas. We proceed in two steps.

Mapping approximate time independent to (exact) time dependent point games. First, we convert an *approximate* cheat-penalised TIPG (penTIPG) into an *(exact) cheat-penalised time dependent point game* (penTDPG). We defer its formal definition to the manuscript but note that it serves a similar purpose here as TDPGs did in the original WCF setting. Unlike a Λ-penTIPG, a **Λ-penTDPG** with bias ϵ is specified by a sequence of n configurations with positive weights $(p_0, p_1, p_2, \ldots, p_n)$ starting with p_0 which is the "initial configuration" and

p_n which is the "final configuration" as in Eq (2). The intermediate configurations are required to satisfy "validity conditions" similar to those of TIPGs. Crucially, each change in configuration, intuitively, corresponds to one round of interaction in the corresponding coin-flipping protocol.

Theorem 2: Mapping approximate penTIPGs to (exact) penTDPGs (simplified, informal)

Let (h, v) be a $(\Lambda, \varepsilon_{\mathsf{approx}})$-penTIPG with bias ϵ. Then, one can construct an (exact) Λ-penTDPG $(p_0, \ldots, p_n)$ with bias $\epsilon + \mathsf{err}$ where the tradeoff between n and err can be tuned using two parameters (details suppressed). However, using these parameters, err can only be made to approach zero if $\varepsilon_{\mathsf{approx}} = 0$. Finally, the number of points in the (exact) penEBM point game $(p_0, \ldots, p_n)$ is at most the number of points in the approximate penTIPG (h, v), i.e., $\max_i\{|\mathsf{supp}(p_i)|\} \leq |\mathsf{supp}\{h, v\}|$.

We emphasise that the above deals with *approximate* point games and that such a reduction is new; it has not been studied in the non-cheat-penalised setting and could find application in other coin-flipping or quantum multiparty frameworks.

Mapping time-dependent point games to protocols. In Miller [Mil20], it was shown that an efficient WCF protocol leads to a point game with small norm (which he shows cannot exist). What we want is the converse in the cheat-penalised setting, point games with small norm lead to efficient protocols—together with explicit bounds on the resources required. While the former is a simple application of the triangle inequality, the latter turns out to be more delicate and involved (even given the point game analysis for standard WCF).

Theorem 3: Mapping time dependent point games to protocols (simplified, informal)

Let $(p_0, \ldots, p_n)$ be a Λ-penTDPG with bias ϵ. Then there exists a Λ-penWCF protocol with the same bias, ϵ, that has round complexity $\mathsf{rc} = 2n$ and space complexity (number of qubits) $\mathsf{sc} = 3 \cdot \lceil \log_2(2\mu + 1) \rceil$ where μ is the greatest number of points in a configuration.

Putting it all together. By combining the above three theorems, we now present our main result.

Main Result: The existence of more efficient, secure cheat-penalised weak coin-flipping

There exist weak coin-flipping protocols with cheat penalty $\Lambda = 0.01$, space complexity (number of qubits) $\mathsf{sc} = 24$ and the following trade-offs between the bias and the round complexity.

More round-efficient than WCF.	Bias $\epsilon = 10^{-8}$, round complexity $\mathsf{rc} = 10^{16}$ (rc is still 1000 times better than any possible non-cheat-penalised WCF protocol with a matching bias)
Constant space with low bias.	Bias $\epsilon = 10^{-10}$, round complexity $\mathsf{rc} = 10^{18}$ (rc is still 10 times better)

To obtain a better trade-off, we use $\Lambda = 1$ below.

Potentially amenable to experiments.	Bias $\epsilon = 0.09$, round complexity $\mathsf{rc} = 25,180$ ($\epsilon < \epsilon_{\mathrm{Moch}}(2) = 1/10$)

Significance. Weak coin-flipping stands out as one of the few cryptographic primitives that admits *unconditional security* in the quantum multiparty setting—a rare property in this field. This alone makes it an essential object of study, and our work shows that it can now be done more efficiently, giving hope that these can be implemented *and used* on real hardware. Moreover, optimal weak coin-flipping protocols are known to underpin a broad class of other cryptographic constructions. In particular, the only known optimal quantum protocols for strong coin-flipping [CK09], bit commitment [CK11], and oblivious transfer [CGS] all critically rely on having access to optimal weak coin-flipping subroutines. As a consequence, the inefficiency of weak coin-flipping directly limits the practicality of these higher-level protocols. By revisiting the question of efficient and secure weak coin-flipping, we not only address an open problem but potentially unlock new avenues for secure quantum multiparty computation. This progress invites a natural follow-up: What other primitives or protocols might benefit from studying their cheat-penalised versions—and how far can we push the boundaries of unconditionally secure, practical quantum cryptography?

References

[ABDR04] A. Ambainis, H. Buhrman, Y. Dodis, and H. Rohrig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259, 2004.

[ACG+14] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias. *SIAM Journal on Computing*, 45(3):633–679, 2014.

[Amb04] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 68(2):398–416, 2004.

[AMMS25] Atul Singh Arora, Carl Miller, Mauro E.S. Morales, and Jamie Sikora. Cheat-penalised quantum weak coin flipping. https://atulsingharora.github.io/penWCF, 2025.

[ARW19] Atul Singh Arora, Jérémie Roland, and Stephan Weis. Quantum weak coin flipping. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 205–216, 2019.

[ATSVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V Vazirani, and Andrew C Yao. Quantum bit escrow. In *Proceedings of the thirty-second annual ACM Symposium on Theory of Computing*, pages 705–714, 2000.

[BB84] Charles H. Bennett and Gilles Brassard. Public-key distribution and coin tossing. In *Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[CGS] André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science*, 2016:13.

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533. IEEE, 2009.

[CK11] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 354–362. IEEE, 2011.

[CK17] André Chailloux and Iordanis Kerenidis. Physical limitations of quantum cryptographic primitives or optimal bounds for quantum coin flipping and bit commitment. *SIAM Journal on Computing*, 46(5):1647–1677, 2017.

[Gan17] Maor Ganz. Quantum leader election. *Quantum Information Processing*, 16(3):73, 2017.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154, 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[Mil20] Carl A Miller. The impossibility of efficient quantum weak coin flipping. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 916–929, 2020.

[MNS09] Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. In *Theory of Cryptography Conference*, pages 1–18. Springer, 2009.

[Moc04] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11. IEEE, 2004.

[Moc05] Carlos Mochon. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72:022341, 2005.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arXiv:0711.4114*, 2007.

[SR01] Robert W. Spekkens and Terry Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):012310, 2001.

[SR02] Robert W Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Physical Review Letters*, 89(22):227901, 2002.