A Note on Key Agreement and Non-Interactive Commitments

Alex Lombardi* Luke Schaeffer†

Abstract

We observe that any key agreement protocol satisfying perfect completeness, regardless of its round complexity, can be used to construct a non-interactive commitment scheme.

This observation simplifies the cryptographic assumptions required for some protocols that utilize non-interactive commitments and removes the need for ad-hoc constructions of non-interactive commitments from specific assumptions such as Learning with Errors.

*MIT. Email: alexjl@mit.edu. Research supported in part by an NDSEG fellowship. Research supported in part by NSF Grants CNS-1350619 and CNS-1414119, and by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts W911NF-15-C-0226 and W911NF-15-C-0236.

†MIT. Email: lrs@mit.edu.

1 Introduction

Commitment schemes [Blu81] are a fundamental building block in cryptography. In this note, we focus on the question of constructing *non-interactive* commitment schemes. If trusted setup (or even a common random string) is allowed, then it is known that one-way functions suffice for this goal [HILL99, Nao91].

In the case of non-interactive commitment *without* setup (which, for the rest of this note, we assume is the goal), it is known that *injective* one-way functions suffice [Blu81, Yao82, GL89]. In addition, a construction is known assuming one-way functions along with the existence of certain *hitting-set generators* [BOV03], but there is no black-box construction of non-interactive commitments from one-way functions [MP12].

Finally, there are two constructions of non-interactive commitments known from concrete assumptions [GHKW17]: namely, either the Learning with Errors (LWE) assumption [Reg05] (with superpolynomial modulus-to-noise ratio[1]) or the Learning Parity with Noise (LPN) asssumption [Ale03] (with standard "public-key" parameters,[2] i.e., noise rate $\frac{1}{\sqrt{n}}$).

Non-interactive commitment schemes are useful for minimizing the round complexity of protocols that require generic commitment as a subroutine. Two recent examples of this are [CGJ19], which uses non-interactive commitments to build k-round malicious MPC from k-round malicious-secure (bidirectional) OT, and [BKP19], which uses non-interactive commitments (and the [GHKW17] LWE-based instantiation thereof) within a construction of 2-message weak zero-knowledge arguments for NP.

The complicated status of which assumptions suffice for non-interactive commitment has caused difficulty in minimizing the assumptions required for such low-round protocols; for example, the [CGJ19] main theorem on 4-round MPC additionally requires the existence of injective OWFs to implement their non-interactive commitment-based building blocks.

Our Contributions. We first note that the LWE-based construction of non-interactive commitments [GHKW17] can be replaced with a simple construction from any public-key encryption scheme that may be folklore. Namely, given a public-key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with perfect decryption correctness, it is possible to commit to a bit b by sampling a pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$ and outputting $(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, b))$. In particular, we note that the perfect correctness of PKE implies that this scheme is perfectly binding even though the committer is allowed to choose pk maliciously. This allows for a simple instantiation from LWE with (small) polynomial modulus-to-noise ratio using Regev encryption [Reg05].

More generally, we show that any secure *key agreement protocol* implies the existence of a non-interactive commitment scheme. This implication holds regardless of the round complexity of the key agreement, but crucially requires that the protocol satisfy perfect completeness. Intuitively, this follows from the fact that the transcript τ of a key agreement protocol is effectively a commitment to the key k being agreed on. We formally write down this construction and prove its correctness in Section 3.

As a consequence of our observation, we see that the main theorem of [CGJ19] can be improved to state that (when considering protocols with perfect completeness) the minimal assumption of k-

[1] Although their construction uses a superpolynomial modulus-to-noise ratio, it appears that a sufficiently large polynomial ratio would suffice for their proof to go through.

[2] A heuristic construction from LPN with higher noise rate is also proposed in [GHKW17], but it currently lacks a secure instantiation.

round (bidirectional) oblivious transfer suffices to construct k-round malicious-secure MPC, without additionally assuming injective one-way functions. This follows from the fact that (even semi-honest) oblivious transfer implies key agreement [GKM+00].

Conclusions. Our observation shows that non-interactive commitments come "for free" in any protocol already making use of a perfectly correct "public-key primitive" (i.e., any primitive that implies key agreement), removing the need for additional generic assumptions, such as injective one-way functions, or concrete assumptions, such as LWE.

It remains an interesting open question whether non-interactive commitments can be constructed generically from key agreement with $1-\mathrm{negl}(n)$ completeness (or even PKE with $1-\mathrm{negl}(n)$ correctness). Any such key agreement protocol can be derandomized to satisfy perfect completeness using the techniques of [BV17], but this requires an additional assumption that already suffices to derandomize the [Nao91] commitment scheme [BOV03].

2 Preliminaries

We say that a function $\delta(n) = \mathrm{negl}(n)$ is $\mathsf{negligible}$ if $\delta(n) = n^{-\omega(1)}$. We say that two distribution ensembles $\{X_n\}$ and $\{Y_n\}$ are computationally indistinguishable (denoted $X \approx_c Y$) if for all polynomial-sized circuit ensembles $\{\mathcal{A}_n\}$, there exists a negligible function $\delta(n)$ such that

$$\left| \Pr\left[\mathcal{A}_n(X_n) = 1\right] - \Pr\left[\mathcal{A}_n(Y_n) = 1\right] \right| \leq O(\delta(n)).$$

2.1 Key Agreement

A key agreement protocol is an efficiently computable protocol Π executed by two parties (that we call Alice and Bob). For a protocol execution in which Alice uses randomness ρ and Bob uses randomness σ, let $\tau = \tau(\rho, \sigma)$ denote the transcript of the execution, let $k_A := k_A(\tau, \rho)$ denote Alice's output, and let $k_B := k_B(\tau, \sigma)$ denote Bob's output. We require that Π satisfies two properties:

- **Perfect Completeness**: $k_A = k_B$ with probability 1 over the randomness (ρ, σ) of the protocol.
- **Passive Security**: the key $k := k_A = k_B$ is computationally pseudorandom given the transcript τ of the protocol. More formally, we require that

  $$\{(\tau, k)\} \approx_c \{(\tau, k')\},$$

  where (τ, k) is sampled according to an honest execution of Π, while k' is sampled uniformly at random (independently of τ).

2.2 Non-Interactive Commitments

A non-interactive commitment scheme Com consists of a single PPT algorithm $\mathsf{Commit}(b; r)$ satisfying two properties:

- **Perfect Binding**: for every pair (r_0, r_1), we have that $\mathsf{Commit}(0; r_0) \neq \mathsf{Commit}(1; r_1)$.

- **Computational Hiding**: the distribution $\{\mathsf{Commit}(0, r_0)\}$ (for uniformly random r_0) is computationally indistinguishable from the distribution $\{\mathsf{Commit}(1, r_1)\}$ (for uniformly random r_1).

3 Construction

Let Π denote a key agreement protocol with perfect completeness. We now define a non-interactive commitment scheme Com using Π by describing the commitment algorithm Commit.

- Input: a bit b and randomness (ρ, σ) for an execution of Π.
- Compute the transcript $\tau = \tau(\rho, \sigma)$ according to Π.
- Output $(\tau, b \oplus k_A(\tau, \rho))$.

We now prove our main result.

Theorem 3.1. *If Π is a perfectly correct, passively secure key agreement protocol, then the scheme Com is a perfectly binding, computationally hiding commitment scheme.*

We prove Theorem 3.1 in two parts.

Lemma 3.2. *If Π satisfies perfect completeness, then Com satisfies perfect binding.*

Proof. Suppose that there exists randomness (ρ_0, σ_0) and (ρ_1, σ_1) such that $\mathsf{Com}(0; \rho_0, \sigma_0) = \mathsf{Com}(1; \rho_1, \sigma_1)$. In particular, this would imply that $\tau(\rho_0, \sigma_0) = \tau(\rho_1, \sigma_1)$. We now further claim that the *mixed* choice of randomness (ρ_1, σ_0) *also* produces the same transcript.

Claim 3.2.1. $\tau(\rho_0, \sigma_0) = \tau(\rho_1, \sigma_0)$.

Proof. We first reformulate the perfect completeness property of Π. By definition of Π, the ith pair of messages (α_i, β_i) can be computed in the following way: $\alpha_i = f_i(\tau_{i-1}, \rho)$ is a deterministic function of the partial transcript τ_{i-1} along with Alice's randomness ρ, while $\beta_i = g_i(\tau_{i-1}, \alpha_i, \sigma)$ is a deterministic function of the partial transcript (τ_{i-1}, α_i) along with Bob's randomness σ. Thus, the equation $\tau(\rho_0, \sigma_0) = \tau(\rho_1, \sigma_1)$ is equivalently the following collection of equations for all $1 \leq i \leq r$:

$$\alpha_i = f_i(\tau_{i-1}, \rho_0) = f_i(\tau_{i-1}, \rho_1) \text{ and}$$

$$\beta_i = g_i(\tau_{i-1}, \alpha_i, \sigma_0) = g_i(\tau_{i-1}, \alpha_i, \sigma_1).$$

Under this formulation, it follows by induction over the rounds that $\tau(\rho_0, \sigma_0) = \tau(\rho_1, \sigma_0)$ as well. □

Finally, by invoking the completeness of Π on (ρ_0, σ_0) and (ρ_1, σ_0), respectively, we conclude that

$$k_A(\tau, \rho_0) = k_B(\tau, \sigma_0) = k_A(\tau, \rho_1)$$

This implies that $k_A(\tau, \rho_0) \neq 1 \oplus k_A(\tau, \rho_1)$, contradicting our assumption. Thus, we conclude that Com is perfectly binding. □

Lemma 3.3. *If Π satisfies passive security, then Com satisfies computational hiding.*

Proof. By the passive security of Π, we know that $(\tau, k_A(\tau, \rho))$ is computationally indistinguishable from (τ, k') for uniformly random k'. Thus, we conclude that for $b \in \{0,1\}$, $\mathsf{Com}(b; \rho, \sigma)$ is computationally indistinguishable from $(\tau(\rho, \sigma), b \oplus k') \equiv (\tau(\rho, \sigma), k')$. The latter distribution is independent of b, so the lemma follows. $\square$

References

[Ale03] Michael Alekhnovich, *More on average case vs approximation complexity*, 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings., IEEE, 2003, pp. 298–307.

[BKP19] Nir Bitansky, Dakshita Khurana, and Omer Paneth, *Weak zero-knowledge beyond the black-box barrier*, Proceedings of the thirty-seventh annual ACM symposium on Theory of computing (STOC 2019), 2019.

[Blu81] Manuel Blum, *Coin flipping by telephone*, Advances in Cryptology–CRYPTO 1981, 1981, pp. 11–15.

[BOV03] Boaz Barak, Shien Jin Ong, and Salil Vadhan, *Derandomization in cryptography*, Annual International Cryptology Conference, Springer, 2003, pp. 299–315.

[BV17] Nir Bitansky and Vinod Vaikuntanathan, *A note on perfect correctness by derandomization*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2017, pp. 592–606.

[CGJ19] Arka Rai Choudhuri, Vipul Goyal, and Abhishek Jain, *On round optimal secure multiparty computation from minimal assumptions*, https://eprint.iacr.org/2019/216.

[GHKW17] Rishab Goyal, Susan Hohenberger, Venkata Koppula, and Brent Waters, *A generic approach to constructing and proving verifiable random functions*, Theory of Cryptography Conference, Springer, 2017, pp. 537–566.

[GKM+00] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan, *The relationship between public key encryption and oblivious transfer*, Proceedings 41st Annual Symposium on Foundations of Computer Science, IEEE, 2000, pp. 325–335.

[GL89] Oded Goldreich and Leonid A Levin, *A hard-core predicate for all one-way functions*, Proceedings of the twenty-first annual ACM symposium on Theory of computing, ACM, 1989, pp. 25–32.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby, *A pseudorandom generator from any one-way function*, SIAM Journal on Computing **28** (1999), no. 4, 1364–1396.

[MP12] Mohammad Mahmoody and Rafael Pass, *The curious case of non-interactive commitments–on the power of black-box vs. non-black-box use of primitives*, Advances in Cryptology–CRYPTO 2012, Springer, 2012, pp. 701–718.

[Nao91] Moni Naor, *Bit commitment using pseudorandomness*, Journal of cryptology **4** (1991), no. 2, 151–158.

[Reg05] Oded Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, ACM, 2005, pp. 84–93.

[Yao82] Andrew C Yao, *Theory and application of trapdoor functions*, 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), IEEE, 1982, pp. 80–91.