A Practical Scheme for String Commitment based on the Gaussian Channel

Frédérique Oggier and Kirill Morozov
Research Center on Information Security
National Institute of Advanced Industrial Science and Technology
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
frederique@systems.caltech.edu,kirill.morozov@aist.go.jp

***Abstract*— We consider the problem of information-theoretically secure string commitment using channel with additive white Gaussian noise. While the current results in the literature mainly present existence results for such schemes, we present here a practical scheme using lattice codes and analyze its security parameters for finite code lengths.**

I. Introduction

Consider the following problem (from [14]): Alice and Bob are playing the final of world chess championship and it is Alice's turn to play. However, it is getting late, and the game will be postponed to the next day. Now if Alice plays, then Bob will have the whole night to think of his next move, giving an unfair disadvantage to Alice. If a trusted referee is present, Alice can tell him her next move, and the referee will keep it secret till the next day. Commitment schemes have been proposed by Blum [4] to solve these kinds of problems without the help of a third trusted party. They have found numerous applications in cryptography, in particular for zero-knowledge proofs (for details, see the tutorial by Damgård and Nielsen [10] and references therein). Commitment schemes consist of two phases: first Alice sends to Bob some information about the data she commits to (for example, her move the next morning), and second, she reveals the committed data (the next morning she actually plays the move she committed to). For this protocol to be secure for both Alice and Bob, the data Alice commits to should be such that Bob cannot learn more than some negligible information about Alice's next move (secure for Alice), but also, such that Alice cannot change her move afterwards (secure for Bob).

We do not make any assumptions on the computational ability of Alice and Bob. In particular, this means that the cheating player may possess unlimited computing power. In this case, assuming only noiseless communications, it is well-known that commitment schemes are impossible [10, Sect 2.3]. In this paper, we will consider the scenario in which Alice and Bob have access to a noisy channel. This point of view has gained interest following the work by Crépeau and Kilian [8]. It was later elaborated by Crépeau [7], who showed that information-theoretically secure bit commitments can be efficiently implemented using a binary symmetric channel. The research that has followed has been directed at constructing commitment schemes using more realistic noise models. Winter et al. [14] extended Crépeau's approach to string commitments [1] for discrete memoryless channels, and the notion of commitment capacity was introduced, as the optimal rate at which a noisy channel can be used for string commitment. In [1], [13], the commitment capacity has been computed for Gaussian channels, and was shown to be infinite. In [3], Bloch et al. investigated a connection between bit commitment and key agreement and provided a methodology for constructing commitment schemes based on noisy channels.

The contribution of this work is to solve an open problem which naturally arises from the previous works [13], [3] – we present a (specific) practical construction of bit commitment schemes based on lattice codes and show that the security failure probabilities decay exponentially in the lattice code length. In particular, we compute a number of parameter sets for specific security requirements.

This paper is organized as follows. We first recall basic definitions related to commitment schemes, and the general methodology used to design bit commitment schemes using noisy channels. We focus on the Gaussian case and recall the channel model for this scenario. Section III contains the main part of this work, namely an explicit lattice code constructions, and well as the computation of security parameters involved in using these codes for bit string commitment.

II. Framework for Gaussian commitment schemes

We start by formalizing the definition of string commitment. We consider two parties, Alice and Bob. Alice picks a message a from a set $\mathcal{A}$ to which she decides to commit to.

1) *Commit phase*: based on $a \in \mathcal{A}$ chosen by Alice, Alice and Bob exchange messages, leading to Alice committing to the chosen a.
2) *Reveal phase*: Alice discloses her chosen $a \in \mathcal{A}$ as well as other relevant information to Bob.

Bob can thus make a test T, based on both the committed data and the revealed data, to either accept the value committed to by Alice if he thinks Alice can be trusted or reject it if he thinks Alice did not follow the protocol.

We now focus on the case where string commitment schemes are implemented with the help of a Gaussian channel

[1] Here, one can commit to a bit string instead of a single bit.

[1], [13]. Alice and Bob have access to two channels: a *noiseless* channel, and an additive white Gaussian noise channel, given by

$$y = x + z,$$

where $x \in \mathbb{R}$ is the sent signal, $z \in \mathbb{R}$ is the Gaussian noise, $z \sim \mathcal{N}(0, \sigma^2)$ and $y \in \mathbb{R}$ is the received signal. When sending a codeword $x^n = (x_1, \ldots, x_n) \in \mathbb{R}^n$ of length n, we have

$$y^n = x^n + z^n \tag{1}$$

where $z^n = (z_1, \ldots, z_n) \in \mathbb{R}^n$ and $z_i \sim \mathcal{N}(0, \sigma^2)$ are i.i.d., $i = 1, \ldots, n$. We assume the power constraint

$$\frac{1}{n} \sum_{i=1}^{n} x_i^2 = P.$$

We denote by d_E the Euclidean distance between two vectors $x^n, y^n \in \mathbb{R}^n$, that is

$$d_E(x^n, y^n) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}.$$

We further assume that an encoder for Gaussian channels is available, that is a mapping from $\{0,1\}^k \to \mathcal{X}^n$, where $\mathcal{X} \subset \mathbb{R}$. Both Alice and Bob have access to the encoder. To describe the scheme, it is enough to assume the existence of such an encoder. We will show later in the paper how to actually construct a practical suitable encoder. Moreover, the players agree to use a 2-universal class of hash functions by Carter and Wegman [5] (their paper provides a number of explicit constructions). We use these functions as a technical tool, hence the details are omitted due to space limitation.

We can now recall the commitment protocol given in [1], [13]. **Gaussian commitment**:

1) Commit phase:
   - Alice randomly chooses a string $w^k \in \{0,1\}^k$, and encodes it into the codeword $x^n \in \mathcal{X}^n$. She then sends x^n to Bob, over the *Gaussian* channel.
   - Alice picks her committed message $a^r \in \mathcal{A}^r$, where r is the bit length of the message (we assume that $r \geq 2$ for string commitment).
   - Alice computes $g(w^k)$, where g is a hash function, $g : \{0,1\}^k \to \{0,1\}^r$, where $k > r > 0$ depends on the chosen function, and g is taken uniformly at random from the 2-universal class. She then computes the r-bit string m^r such that $g(w^k) \oplus m^r = a^r$, where $\oplus$ denotes the bitwise XOR. She sends m^r and g over the *noiseless* channel.
2) Reveal phase: Alice sends w^k to Bob, over the *noiseless* channel. Since Bob already knows g and m^r, he can recover a^r. In order to decide whether he received a valid commitment a^r, Bob uses the encoder to compute x^n, and then checks whether $d_E(x^n, y^n) \leq \sqrt{n(\sigma^2 + \epsilon')}$, for some $\epsilon' > 0$ decided in advance by Alice and Bob.

In order to check that this protocol is actually secure for both Alice and Bob, two properties need to be checked (note that these properties are enunciated in particular for the above protocol):

1) *Concealing* (or *hiding*): after the commitment phase, Bob cannot get any non-negligible amount of information on the value Alice committed to. Formally, a protocol is called ϵ-*concealing* if
$$I(G(W^k); G, Y^n) \leq \epsilon,\ \epsilon > 0,$$
where I denotes the mutual information. The random variables G, W^k, Y^n model respectively the choice of a hash function g in the 2-universal class, the choice of a string w^k in $\{0,1\}^k$, and the output of the Gaussian channel when x^n is given as input (x^n is the codeword that encodes w^k).
2) *Correctness* (or *soundness*) : if both Alice and Bob are honest, we would like the protocol to be successful with high probability. Formally, we say that a protocol is δ-*correct* if
$$\Pr(T(y^n; w^k) = \text{ACC}) \geq 1 - \delta,\ \delta > 0,$$
for all choices of $w^k \in \{0,1\}^k$. Since Bob receives w^k from Alice during the reveal phase and has access to the encoder, we may equivalently write
$$\Pr(T(y^n; x^n) = \text{ACC}) \geq 1 - \delta,\ \delta > 0,$$
for all possible choices of codewords $x^n \in \mathcal{C}$, where y^n is the output of the Gaussian channel, when x^n is given as input.
3) *Binding*: in order for the protocol to be secure for Bob, we need to make sure that Alice cannot change her mind and reveal a value which is different from the value she committed to. Formally, a protocol is η-binding if Bob makes a test T on what he received from Alice during both phases $T(Y^n; w^k)$, and the probability that he accepts both this test and another test $T(Y^n; w'^k)$ is smaller than η:
$$\Pr(T(Y^n; W^k) = \text{ACC} \ \wedge\ T(Y^n; W'^k) = \text{ACC}) \leq \delta,$$
$$\delta > 0,\ w^k \neq w'^k \in \{0,1\}^k.$$
Similarly to above, since Bob receives w^k from Alice and has access to the encoder, we can rewrite
$$\Pr(T(Y^n; x^n) = \text{ACC} \ \wedge\ T(Y^n; x'^n) = \text{ACC}) \leq \delta,$$
$$\delta > 0,\ x^n \neq x'^n \in \mathcal{C}.$$
Note that any sequence w^k Alice may send during the reveal phase will yield a valid codeword x^n. However, during the commit phase, Alice may send any n-string she likes, so that Y^n is any possible output of the Gaussian channel.

In [1], [13], the above Gaussian commitment scheme has been proved to be concealing, binding and correct with two different constructions: a typical sequence encoder in [1] and random codes on the surface of a hypersphere in [13]. Following Crépeau's approach [7], these proofs require the use of *privacy amplification* (see, e.g., the work by Bennett et al. [2]), the concept which we now recall below.

Let W^k be a random variable uniformly distributed over $\{0,1\}^k$, and let Y^n be a continuous random variable obtained from the codeword X^n (encoding W^k) through an additive white Gaussian noise channel as described in (1). Let G be a random variable taking values $g : \{0,1\}^k \to \{0,1\}^r$ uniformly distributed from a class of 2-universal hash functions. The following result has been shown in [13].

Theorem 1: **(Privacy amplification.)** We have that

$$H(G(W^k)|G, Y^n) \geq r - \frac{2^{r-H_\infty(W^k|Y^n)}}{\ln 2}$$

where H_∞ denotes the min-entropy. Furthermore, in the case of the Gaussian channel we consider, we have that

$$H_\infty(W^k|Y^n) \geq H(W^k) - nC - n\delta',$$

for any $\delta' > 0$, where C denotes the capacity of the channel. Note that the above result holds for asymptotic n (i.e., $n \to \infty$), and uses the fact that

$$H_\infty(W^k|Y^n) = \lim_{\epsilon \to 0} H_\infty^{\epsilon''}(W^k|Y^n)$$

where $H_\infty^{\epsilon''}$ denotes the ϵ''-min entropy. To deal with the case where n is finite, we refer to [11, Thm 1], where it has been shown that

$$H_\infty^{\epsilon''}(W^k|Y^n) \geq H(W^k|Y^n) - n\delta',$$

with

$$\epsilon'' = 2^{\frac{-n\delta'^2}{2\log^2 5}}.$$

III. A LATTICE CODE BASED SCHEME

In this section, we now describe an encoder based on lattice codes, in order to implement a practical bit commitment scheme.

A. A family of lattice codes

Recall that a lattice Λ is a discrete subgroup of $\mathbb{R}^n$, that can for example be given by its generator matrix M:

$$\Lambda = \{\mathbf{x} \in \mathbb{R}^n,\ \mathbf{x} = M\mathbf{u},\ \mathbf{u} \in \mathbb{Z}^n\}.$$

A lattice code can be obtained using the so-called *construction A* [6, p.137],[12] as follows. Let C be an (n, k_c, d) binary linear code, that is a binary error correcting code of length n, dimension k_c and minimum distance d. Then a lattice code $\mathcal{C}_\infty(\Lambda)$ is defined by

$$\mathcal{C}_\infty(\Lambda) = \{\mathbf{x} = 2\mathbf{x}' + c,\ \mathbf{x}' \in \mathbb{Z}^n,\ c \in C\}.$$

Note that the binary code is embedded in $\mathbb{R}^n$, and that $\mathcal{C}_\infty$ is clearly an infinite code.

Example. A famous example of this code construction is given in dimension 8, by considering the code $C = (8, 4, 4)$. It can be shown that the resulting construction is isomorphic to the lattice E_8.

In order to obtain a finite codebook, we restrict the coefficients of $\mathbf{x}'$ from $\mathbb{Z}^n$ to a bounded set S, that is $S = \{0, 1, \ldots, m-1\}^n$. Thus, we have

$$\mathcal{C}_S(\Lambda) = \{\mathbf{x} = 2\mathbf{x}' + c,\ \mathbf{x}' \in S \subset \mathbb{Z}^n,\ c \in C\} \qquad (2)$$

such that

$$\mathcal{C}_S(\Lambda) \subset \{0, 1, \ldots, 2m-1\}^n.$$

Thus the number of bits required to label one point of $\mathcal{C}_S(\Lambda)$ is $n\lceil \log_2(m) \rceil + k_c$, where k_c is the number of bits necessary to choose one codeword in C, so that the rate R, given in bits per dimension, is

$$R = \lceil \log_2(m) \rceil + \frac{k_c}{n}.$$

It clearly depends on the power P available at the transmitter, which will determine the choice of m, and on the code C.

Let us now look at the minimum distance of the code $\mathcal{C}_S(\Lambda)$. If two codewords in $\mathcal{C}_S(\Lambda)$ are congruent to the same codeword $c \in C$, then their distance apart is at least 2. This is clear, since if two distinct codewords x_1, x_2 are congruent to the same codeword c, then $x_1 = 2x_1' + c$, $x_2 = 2x_2' + c$, so that $d_E(x_1, x_2) = ||x_2 - x_1|| = 2||x_2' - x_1'|| \geq 2$ since $x_1', x_2' \in \mathbb{Z}$ and $x_1 \neq x_2$. Now if they are congruent to different codewords $c \neq c' \in C$, then by definition of C, they differ by at least 1 in at least d coefficients, and so are at least of distance $\sqrt{d}$ apart. Thus the minimum distance $d(\Lambda)$ is

$$d(\Lambda) = \min(2, \sqrt{d}).$$

Summarizing the above considerations, we have

Lemma 1: Let C be an (n, k_c, d) binary linear code. Then the code $\mathcal{C}_S(\Lambda)$ defined in (2) has rate $R = \lceil \log_2(m) \rceil + \frac{k_c}{n}$ and minimum distance $\min(2, \sqrt{d})$.

Note that all the points of the code $\mathcal{C}_S(\Lambda)$ are inside an n-dimensional box of edge $2m$. Thus they are all inside an n-dimensional sphere of radius $\sqrt{n}m$. In other words, if we have a power constraint of P, that means that all codewords have to lie inside a sphere of radius $\sqrt{nP}$, meaning that for this particular construction, points are within a box with each edge of length $2\sqrt{P}$. As a function of the power P, there is thus a tradeoff between rate and minimum distance. In order to have a minimum distance of $d(\Lambda) = \min(2, \sqrt{d})$, then the rate is $R(P) = \lceil \log_2(\sqrt{P}) \rceil + \frac{k_c}{n}$. Vice versa, in order to increase the rate, the minimum distance will be reduced. If $m = N\sqrt{P}$, then the minimum distance is similarly scaled by N: $d(\Lambda) = \frac{\min(2, \sqrt{d})}{N}$. Thus more generally, for $m = M$, the minimum distance is $d(\Lambda) = \frac{\sqrt{P}}{M} \min(2, \sqrt{d})$.

B. Lattice codes for commitment schemes

We now consider a Gaussian string commitment scheme with the lattice encoder discussed above.

This first lemma essentially comes from [13]. Recall that C is the capacity of the channel and r is the size of the hash function g output.

Lemma 2: **(Concealing.)** Let $\mathcal{C}$ be a code that encodes a message $w^k \in \{0,1\}^k$ into a codeword $x^n \in \mathcal{X}^n$, thus of rate $R = k/n$. If

$$r \leq k\left(1 - \frac{1}{R}(C + \delta') - \gamma\right) \qquad (3)$$

for some $\gamma > 0$, and some δ' as in the proof, then

$$I(G(W^k); G, Y^n) \leq 2^{-k\gamma} / \ln 2,$$

where W^k, Y^n and G are random variables whose realizations are respectively w^k, y^n, g. Note that (3) means that $\frac{k(1-\gamma)}{n} \geq C + \frac{r}{n} + \delta'$, and in particular the code we use is not good enough for Bob to be able to decode y^n.

Proof: We have by definition that

$$\begin{aligned} I(G(W^k); G, Y^n) &= H(G(W^k)) - H(G(W^k)|G, Y^n) \\ &\leq 2^{r - H_\infty(W^k|Y^n)}/\ln 2 \end{aligned}$$

using Theorem 1 and the fact that $H(G(X^n)) = r$. Now again using Theorem 1, we have that

$$-H_\infty(W^k|Y^n) \leq -(H(W^k) - nC - n\delta') = -k + \frac{k}{R}(C + \delta'),$$

for some $\delta' > 0$, which, combined with (3), yields the result. ∎

Corollary 1: If $R = \lceil \log_2(m) \rceil + \frac{k_c}{n}$, then the protocol is ϵ-concealing, with

$$\epsilon = 2^{-\gamma(n\lceil \log_2(m) \rceil + k_c)}/\ln 2.$$

Note that when n grows, ϵ decays exponentially in n.

Lemma 3: **(Correctness.)** The protocol is δ-correct, that is

$$\Pr(T(y^n; w^k) = \text{ACC}) \geq 1 - \delta,$$

with

$$\delta = e^{-n\left(\frac{\epsilon'}{2\sigma^2}\right)} \left(\frac{\sigma^2 + \epsilon'}{\sigma^2}\right)^{n/2}.$$

In particular, since

$$e^{\frac{-\epsilon'}{2\sigma^2}} \sqrt{1 + \frac{\epsilon'}{\sigma^2}} < 1, \ \epsilon' > 0,$$

then δ decays exponentially in n if $\epsilon' > 0$.

Proof: By definition of the test T performed by Bob, we have

$$\begin{aligned} & \Pr(T(y^n; w^k) = \text{ACC}) \\ = \ & \Pr(T(y^n; x^n) = \text{ACC}) \\ = \ & \Pr(d_E(x^n, y^n) \leq \sqrt{n(\sigma^2 + \epsilon')}) \\ = \ & 1 - \Pr(d_E(x^n, y^n)^2 \geq n(\sigma^2 + \epsilon')). \end{aligned}$$

Since $d_E(x^n, y^n)^2 = \sum_{i=1}^n z_i^2$ and using the Chernoff bound, we get

$$\begin{aligned} & \Pr(T(y^n; w^k) = \text{ACC}) \\ \geq \ & 1 - e^{-\lambda n(\sigma^2 + \epsilon')} E[e^{\lambda \sum_{i=1}^n z_i^2}] \\ = \ & 1 - (e^{-\lambda(\sigma^2 + \epsilon')} E[e^{\lambda z^2}])^n \end{aligned}$$

for $\lambda > 0$ and some $z \sim \mathcal{N}(0, \sigma^2)$ since $z_1, \ldots, z_n$ are $i.i.d.$ Now we have that

$$\begin{aligned} E[e^{\lambda z^2}] &= \frac{1}{\sqrt{2\pi\sigma^2}} \int e^{\lambda z^2} e^{-z^2/(2\sigma^2)} dz \\ &= \frac{1}{\sqrt{1 - 2\sigma^2\lambda}} \end{aligned} \quad (4)$$

by setting σ' such that $\frac{1 - 2\lambda\sigma^2}{\sigma^2} = \frac{1}{\sigma'^2}$. Thus

$$\Pr(T(y^n; w^k) = \text{ACC}) \geq 1 - \left(\frac{e^{-\lambda(\sigma^2 + \epsilon')}}{\sqrt{1 - 2\lambda\sigma^2}}\right)^n \quad (5)$$

for $\lambda > 0$. We now optimize on λ, that is compute the derivative to find that $1 - 2\lambda\sigma^2 = \sigma^2/(\sigma^2 + \epsilon')$, that is,

$$\lambda = \frac{\epsilon'}{2\sigma^2(\epsilon' + \sigma^2)}.$$

This concludes the proof, by replacing λ in (5). ∎

Lemma 4: **(Binding.)** The protocol is η-binding, that is

$$\Pr(T(Y^n; w^k) = \text{ACC} \ \wedge \ T(Y^n; w'^k) = \text{ACC}) \leq \eta,$$

with

$$\eta = \left(1 - \frac{\epsilon'}{\sigma^2 + d(\Lambda)^2/4n}\right)^{n/2} e^{\frac{n\epsilon'}{2(\sigma^2 + d(\Lambda)^2/4n)}},$$

$w^k \neq w'^k$. In particular, the bound decreases exponentially in n.

Proof: Since for a given input x^n, the output y^n of the channel will be uniformly distributed inside a ball of radius $\sqrt{n\sigma^2}$, the best strategy for Alice to cheat is to send a sequence $\bar{x}^n$ between two valid codewords x^n and x'^n (i.e., $\bar{x}^n$ is both equidistant and as close as possible to either of them). Note that for one of these two codewords, say x^n, we have that

$$d_E(\bar{x}^n, x^n) \geq d(\Lambda)/2,$$

where $d(\Lambda)$ is the minimum distance of the code. Note that on average, such a sequence $\bar{x}^n$ can be seen as the output of a Gaussian channel with suitable noise variance $\bar{\sigma}^2$, that is

$$\bar{x}^n = x^n + \bar{z}^n, \ \bar{z}_i \sim \mathcal{N}(0, \bar{\sigma}^2), \ \bar{\sigma}^2 \geq d(\Lambda)^2/4n,$$

since

$$E[d_E(x^n, x^n + \bar{z}^n)^2] = \sum_{i=1}^n E[\bar{z}_i^2] \geq d(\Lambda)^2/4.$$

Let now $d_E(\bar{x}^n + z^n, x^n)$ be the distance between a legal codeword x^n and the output of the channel, when the illegal n-string $\bar{x}^n$ is fed, which has been chosen randomly between x^n and x'^n. In order to evaluate whether Alice is cheating, Bob now uses the fact that

$$\begin{aligned} & E[d_E(\bar{x}^n + z^n, x^n)^2] \\ = \ & E[d_E(x^n + \bar{z}^n + z^n, x^n)^2] \\ = \ & E[||\bar{z}^n + z^n||^2] \\ = \ & E[||\tilde{z}^n||^2], \ \tilde{z}_i \sim \mathcal{N}(0, \sigma^2 + \bar{\sigma}^2) \\ \geq \ & n\sigma^2 + d(\Lambda)^2/4, \end{aligned}$$

that is, if Alice is cheating, on average the received word will be at distance $n\sigma^2 + d(\Lambda)^2/4$ from a valid codeword. To conclude the proof, it is thus enough to show that the probability of sending a n-string $\bar{x}^n$ in between two valid codewords x^n and x'^n and being far from this average is exponentially small in n. We have that

$$\begin{aligned} & \Pr(d_E(\bar{x}^n + z^n, x^n)^2 \leq n\sigma^2 + d(\Lambda)^2/4 - n\epsilon') \\ = \ & \Pr(e^{-\lambda||\tilde{z}^n||^2} \geq e^{-\lambda(n\sigma^2 + d(\Lambda)^2/4 - n\epsilon')}) \\ \leq \ & \frac{E[e^{-\lambda||\tilde{z}^n||^2}]}{e^{-\lambda(n\sigma^2 + d(\Lambda)^2/4 - n\epsilon')}} \\ = \ & \left(\frac{E[e^{-\lambda\tilde{z}^2}]}{e^{-\lambda(\sigma^2 + d(\Lambda)^2/4n - \epsilon')}}\right)^n \end{aligned}$$

for some $\lambda > 0$ using Markov inequality, and where $\tilde{z} \sim \mathcal{N}(0, \tilde{\sigma}^2)$, $\tilde{\sigma}^2 \geq \sigma^2 + d(\Lambda)^2/4n$. Now we have as in (4) that

$$E[e^{-\lambda \tilde{z}^2}] = \frac{1}{\sqrt{1+2\tilde{\sigma}^2\lambda}}.$$

Thus we have

$$\begin{aligned} & \Pr(d_E(\bar{x}^n + z^n, x^n)^2 \leq n(\sigma^2 - \epsilon') + d(\Lambda)^2/4) \\ \leq & \left(\frac{1}{\sqrt{1+2\tilde{\sigma}^2\lambda}} e^{\lambda(\sigma^2 + d(\Lambda)^2/4n - \epsilon')} \right)^n \\ \leq & \left(\frac{1}{\sqrt{1+2\lambda(\sigma^2 + d(\Lambda)^2/4n)}} e^{\lambda(\sigma^2 + d(\Lambda)^2/4n - \epsilon')} \right)^n \end{aligned}$$

by definition of $\tilde{\sigma}^2$. Set

$$\alpha = \sigma^2 + d(\Lambda)^2/4n.$$

We now optimize over λ as before, and find that

$$\lambda = \frac{\epsilon'}{2\alpha(\alpha - \epsilon')},$$

which yields that

$$\begin{aligned} & \Pr(d_E(\bar{x}^n + z^n, x^n)^2 \leq n(\sigma^2 - \epsilon') + d(\Lambda)^2/4) \\ \leq & \left(\sqrt{1 - \frac{\epsilon'}{\alpha}} e^{\frac{\epsilon'}{2\alpha}} \right)^n. \end{aligned}$$

■

IV. Conclusion

We presented the information-theoretic string commitment based on the Gaussian channel and employing the lattice codes. These codes suits our purpose well as they provide an efficient embedding of (good) binary error-correcting codes to the real n-dimensional plane. Our scheme is, to the best of the authors' knowledge, the first practical scheme which is proposed for this scenario. We have analyzed it for finite code length and derived the security parameters explicitly. In particular, we have shown that the security failure probabilities decrease exponentially fast in the code length. Optimizing those parameters for obtaining the achievable commitment rates is a matter of our ongoing work.

We would like to propose as an open question providing commitment schemes for more realistic noise models: Gaussian channels with memory and fading channels. From the theoretical point of view, of great interest is defining the so-called *unfairness* in the spirit of [9] for the Gaussian channels and building the schemes secure in this model.

References

[1] J. Barros, H. Imai, A.C.A Nascimento, S. Skludarek, "Bit Commitment over Gaussian Channels", Proc. ISIT '06, pp. 1437–1441, IEEE, 2006.

[2] C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[3] M. Bloch, J. Barros, S.W. McLaughlin, "Practical Information-Theoretic Commitment," To appear in Proc. 45th Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, September 2007.

[4] M. Blum, "Coin flipping by telephone: a protocol for solving impossible problems," *Proc. IEEE Computer Conference*, pp. 133–137, 1982.

[5] J.L. Carter, M.N. Wegman, "Universal Classes of hash functions," *J. of Computer and Syst. Sci.*, vol. 18, pp. 143–154, 1979.

[6] J.H. Conway, N.J.A. Sloane "Sphere packings, lattices and groups", 3rd edition, *Springer Verlag*, 1999.

[7] C. Crépeau, "Efficient Cryptographic Protocols Based on Noisy Channels," *Proc. EUROCRYPT '97*, LNCS, vol. 1233, pp. 306–317, 1997.

[8] C. Crépeau, J. Kilian, "Achieving oblivious transfer using weakened security assumptions," *Proc. 29th FOCS, IEEE*, pp. 42–52, 1988.

[9] I. B. Damgård, J. Kilian, L. Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions", *Proc. EUROCRYPT '99*, LNCS, vol. 1592, pp. 56–73, 1999.

[10] I. Damgård, J. Nielsen, "Commitment Schemes and Zero-Knowledge Protocols", 2007. Available at: http://www.daimi.au.dk/ivan/ComZK07.pdf

[11] T. Holenstein and R. Renner, "On the Randomness of Independent Experiments," Pre-print, August 2006. Available at http://arxiv.org/abs/cs.IT/0608007

[12] Y. Hong, E. Viterbo and J.-C. Belfiore, "Golden Space-Time Trellis Coded Modulation," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1689–1705, May 2007.

[13] A.C.A. Nascimento, S. Skludarek, J. Barros, H. Imai, "The Commitment Capacity of the Gaussian Channel is Infinite," Accepted to *IEEE Trans. on Information Theory, Special Issue on Information Security*, November 2007.

[14] A. Winter, A. C. A. Nascimento, H. Imai, "Commitment Capacity of Discrete Memoryless Channels", *Proc. 9th IMA International Conf. on Cryptography and Coding*, LNCS, vol. 2898, pp. 35–51, 2003.