NTNU | Norwegian University of Science and Technology

SHORT PAPER: VERIFIABLE DECRYPTION FOR BGV

7th Workshop on Advances in Secure Electronic Voting

Tjerand Silde. April, 2022. Slides: tjerandsilde.no/files/voting.pdf

Introduction - Goal

A verifiable decryption protocol is a zero-knowledge protocol proving that a certain message is the correct decryption of a certain ciphertext with respect to a committed key which does not reveal anything about the decryption key.

Verifiable decryption is crucial to prove correct outcome in electronic voting. Today's systems use discrete logs, and can be broken by quantum computers.

Goal: design an efficient verifiable decryption protocol for lattice cryptography.

Introduction - Contribution

We analyze the most developed lattice-based protocols in the literature, combine them into a verifiable decryption protocol and argue its security.

We give parameters and a prototype implementation proving its practicality.

We conduct a comparison to verifiable decryption protocols in the literature.

Introduction - Building Blocks

- Encryption scheme with linear decryption (Brakerski *et al.* [BGV12])
- Commitment scheme with proofs of linearity (Baum *et al.* [BDL+18])
- Amortized proofs of bounded values (Baum *et al.* [BBC+18])

Background - BGV Encryption (Brakerski *et al.* [BGV12])

Let $p \ll q$ be primes, R_q and R_p be polynomial rings with fixed dimension N, $\mathtt{D}$ be a bounded distribution over R_q, and let $\beta_\infty \in \mathbb{N}$ be a bound.

- KGen samples $a \leftarrow\!\!\$\ R_q$ uniformly at random, samples a short $s \leftarrow\!\!\$\ S_{\beta_\infty}$ and samples noise $e \leftarrow \mathtt{D}$. It outputs keys $\mathtt{pk} = (a, b) = (a, as + pe)$ and $\mathtt{sk} = s$.
- Enc, on input pk and a message m in R_p, samples a short $r \leftarrow\!\!\$\ S_{\beta_\infty}$, samples noise $e', e'' \leftarrow \mathtt{D}$, and outputs ciphertext $c = (u, v) = (ar + pe', br + pe'' + m)$.
- Dec, on input $\mathsf{sk} = s$ and $c = (u, v)$, outputs $m = (v - su \mod q) \mod p$.

The Dec algorithm outputs correct message if $B_{\mathtt{Dec}} = \max\|v - su\|_\infty < \lfloor q/2 \rfloor$.

Background - Commitments (Baum *et al.* [BDL+18])

- KGen outputs a public key $\mathtt{pk} = \boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{a}_2 \end{bmatrix}$ where

$$\begin{aligned} \boldsymbol{A}_1 &= \begin{bmatrix} \boldsymbol{I}_n & \boldsymbol{A}'_1 \end{bmatrix} && \text{where } \boldsymbol{A}'_1 \leftarrow\!\!\$\; R_q^{n\times(k-n)} \\ \boldsymbol{a}_2 &= \begin{bmatrix} 0^n & 1 & \boldsymbol{a}'_2 \end{bmatrix} && \text{where } \boldsymbol{a}'_2 \leftarrow\!\!\$\; R_q^{(k-n-1)}, \end{aligned}$$

- Com commits to messages $m \in R_q$ by sampling $\boldsymbol{r}_m \leftarrow\!\!\$\; S^k_{\beta_\infty}$, and computes

$$\mathtt{Com}_{\mathtt{pk}}(m; \boldsymbol{r}_m) = \boldsymbol{A} \cdot \boldsymbol{r}_m + \begin{bmatrix} 0 \\ m \end{bmatrix} = \begin{bmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \end{bmatrix} = [\![m]\!].$$

- Open verifies opening $(m, \boldsymbol{r}_m, f)$ by checking that $\|\boldsymbol{r}_m\|_2$ is short and that

$$f \cdot \begin{bmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \end{bmatrix} \stackrel{?}{=} \boldsymbol{A} \cdot \boldsymbol{r}_m + f \cdot \begin{bmatrix} 0 \\ m \end{bmatrix}.$$

  Open outputs 1 if all these conditions holds, and 0 otherwise.

Background - Proof of Linearity (Baum *et al.* [BDL+18])

Let $[\![y]\!], [\![y']\!]$ be commitments as above such that $y' = \alpha y + \beta$ for some public values $\alpha, \beta \in R_q$. The protocol Π_{Lin} in [BDL+18] is a zero-knowledge proof of knowledge, with ℓ_2 bound $B_{\mathrm{C}} = 2\sigma_{\mathrm{C}}\sqrt{N}$ on the responses $\boldsymbol{z}_i$, for the relation:

$$\mathcal{R}_{\mathrm{Lin}} = \left\{ (x, w) \;\middle|\; \begin{array}{l} x = (\alpha, \beta, [\![y]\!], [\![y']\!]), w = (y, \boldsymbol{r}_y, \boldsymbol{r}_{y'}, f, f') : \\ \mathtt{Open}([\![y]\!], y, \boldsymbol{r}_y, f) = \mathtt{Open}([\![y']\!], \alpha \cdot y + \beta, \boldsymbol{r}_{y'}, f') = 1 \end{array} \right\}.$$

We get proof $\pi_L = (c, \boldsymbol{z}_1, \boldsymbol{z}_2)$, where each $\boldsymbol{z}_i$ can be compressed to get a proof of size $2(k-n)N\log_2(6\sigma_{\mathrm{C}})$ bits by checking an approximate equality [ABG+21].

Background - Proof of Shortness (Baum *et al.* [BBC+18])

Let $\boldsymbol{A}$ be a public matrix over R_q, let $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_\tau$ be bounded vectors in R_q^{k+1} and let $\boldsymbol{A}\boldsymbol{s}_i = \boldsymbol{t}_i$ for $i \in [\tau]$. Let $\boldsymbol{S}$ be the matrix whose columns are $\boldsymbol{s}_i$ and similar for $\boldsymbol{T}$. We have a zero-knowledge proof of knowledge for the relation:

$$\mathcal{R}_{\mathsf{A}} = \left\{ (x, w) \;\middle|\; \begin{array}{c} x = (\boldsymbol{A}, \boldsymbol{T}), w = \boldsymbol{S} : \\ \forall i \in [\tau] : \ \boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{s}_i \wedge ||\boldsymbol{s}_i||_2 \leq 2 \cdot B_{\mathsf{A}} \end{array} \right\}$$

We get a proof of the form $\pi_{\mathsf{A}} = (\boldsymbol{C}, \boldsymbol{Z})$, where the verification bound on each column of $\boldsymbol{Z}$ is $B_{\mathsf{A}} = \sqrt{2vN}\sigma_{\mathsf{A}}$. Here, σ_{A} and B_{A} depends on the 1-norm of $\boldsymbol{S}$, and hence, the bound depends on the number of equations in the statement.

Protocol - Verifiable Decryption

The verifiable decryption protocol Π_{Dec}, for prover $\mathcal{P}$, goes as following:

1. $\mathcal{P}$ takes as input a set of ciphertexts $(u_1, v_1), \ldots, (u_\tau, v_\tau)$ and $([\![s]\!], s, \boldsymbol{r}_s, f_s)$.
2. $\mathcal{P}$ runs `Dec` on input s and (u_i, v_i) for all $i \in [\tau]$ to obtain $m_1, \ldots, m_\tau$.
3. $\mathcal{P}$ extracts noise d_i by computing $d_i = (v_i - m_i - u_i s)/p \mod q$ for all $i \in [\tau]$.
4. $\mathcal{P}$ commits to all d_i as $[\![d_i]\!]$, and proves $p[\![d_i]\!] = v_i - m_i - u_i[\![s]\!]$ using Π_{Lin}.
5. $\mathcal{P}$ uses protocol Π_{A} to prove that all $\|d_i\|_2$ are bounded by $B_{\text{A}} \leq \sqrt{2vN}\sigma_{\text{A}}$.
6. $\mathcal{P}$ outputs messages $\{m_i\}_{i=1}^{\tau}$, commitments $\{[\![d_i]\!]\}_{i=1}^{\tau}$, proofs $\{\pi_{L_i}\}_{i=1}^{\tau}, \pi_{\text{A}}$.

Conclusion - Results

Message m_i	Ciphertext (u_i, v_i)	Commitment $[\![d_i]\!]$	Proof π_{L_i}	Proof π_{A}	Proof π_{Dec}
0.256 KB	25.6 KB	25.6 KB	19 KB	2.4τ KB	47τ KB

Table: Sizes for params $p = 2, q \approx 2^{50}$ and $N = 2048$ for proof $\pi_{\mathrm{Dec}} = (\{[\![d_i]\!], \pi_{L_i}\}_{i=1}^{\tau}, \pi_{\mathrm{A}})$, where shortness proofs π_{A} is amortized over batches of size $\tau = 2048$. Abort prob: $2/3$.

Noise $[\![d_i]\!]$	Proof Π_{Lin}	Verification Π_{LinV}	Proof Π_{A}	Verification Π_{AV}	Proof π_{Dec}
6 ms	59 ms	15 ms	25τ ms	12τ ms	90τ ms

Table: Amortized time per instance over $\tau = 2048$ ciphertexts. Abort probability: $2/3$. The prototype code is available online at: github.com/tjesi/verifiable-decryption-BGV.

Conclusion - Comparison

- Lyubashevsky *et al.* [LNS21] give a verifiable decryption protocol for the Kyber encapsulation scheme for a ring of dimension $N = 256$ and modulus $q = 3329$ with secret and noise values bounded by $\beta_\infty = 2$. The proof of correct decryption is of size 43.6 KB. They do not provide timings.
- Gjøsteen *et al.* [GHM+21] give a verifiable decryption protocol for BGV. Their proof size is depending on the soundness parameter λ, giving a proof of size 16λ KB per ciphertext. They do not provide (real) timings.
- Boschini *et al.* [BCOS20] give proof sizes of approximate 90 KB, which is roughly twice the size of π_{Dec}. The run time is several minutes per ciphertext, which would deem it unusable for larger sets of ciphertexts.

Conclusion - Remarks

- A more tight analysis and size-timing trade-offs can give smaller proofs.
- Our protocol use lattices for quantum-security, but proof is in ROM.
- Our paper is available on IACR ePrint: eprint.iacr.org/2021/1693.pdf.

Thank you! Any questions?

tjerand.silde@ntnu.no

NTNU | Norwegian University of Science and Technology

Diego F. Aranha, Carsten Baum, Kristian Gjøsteen, Tjerand Silde, and Thor Tunge.
Lattice-based proof of shuffle and applications to electronic voting.
In Kenneth G. Paterson, editor, *CT-RSA 2021*, volume 12704 of *LNCS*, pages 227–251. Springer, Heidelberg, May 2021.

Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky.
Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits.
In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 669–699. Springer, Heidelberg, August 2018.

Cecilia Boschini, Jan Camenisch, Max Ovsiankin, and Nicholas Spooner.
Efficient post-quantum SNARKs for RSIS and RLWE and their applications to privacy.

In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 247–267. Springer, Heidelberg, 2020.

Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert.
More efficient commitments from structured lattice assumptions.
In Dario Catalano and Roberto De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 368–385. Springer, Heidelberg, September 2018.

Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan.
(Leveled) fully homomorphic encryption without bootstrapping.
In Shafi Goldwasser, editor, *ITCS 2012*, pages 309–325. ACM, January 2012.

Kristian Gjøsteen, Thomas Haines, Johannes Müller, Peter Rønne, and Tjerand Silde.
Verifiable decryption in the head.
Cryptology ePrint Archive, Report 2021/558, 2021.

https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2021/558&version=20210503:201150&file=558.pdf.

Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler.
Shorter lattice-based zero-knowledge proofs via one-time commitments.
In Juan Garay, editor, *PKC 2021, Part I*, volume 12710 of *LNCS*, pages 215–241. Springer, Heidelberg, May 2021.