BG14

January 2020

1 Introduction

I just love breaking thing so much!

2 Preliminaries

2.1 Basic notation

Let $q \in \mathbb{N}$ be a prime. We use $\mathbb{Z}_q^n$ to denote the finite field of $\mathbb{Z}_q$ elements. Vectors are represented in bold face as $\mathbf{v} = (v_1, v_2, \ldots, v_n)^T$ and matrices in bold face as $\mathbf{A}$. The inverse matrix of an invertible matrix $\mathbf{A}$ is denoted as $\mathbf{A}^{-1}$. $\mathcal{B}_{k,w}$ is the set of length k vectors of weight w with coefficients in $\{-1, 0, 1\}$. The Euclidean norm is $\|\mathbf{v}\| = \sum_{i=1}^{n} v_i^2$ and the infinity norm (or sup norm) is $\|\mathbf{c}\|_\infty = \max_{1 \leq i \leq n} v_i$.

Let $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, $[a]_{2^d}$ is denoted as the unique integer in $(-2^{d-1}, 2^{d-1}]$ satisfy that $a \equiv [a]_{2^d} \pmod{2^d}$ and $a \in \mathbb{Z}$. Define $\lfloor a \rceil_d = (a - [a]_{2^d})/2^d$ and let $\lfloor a \rceil_d$ be the most significant bit of a after get rid of the d least significant bits. For each vectors $\mathbf{v} = (v_1, v_2, \ldots, v_m) \in \mathbb{Z}^m$ we define $\lfloor \mathbf{v} \rceil_d = (\lfloor v_1 \rceil_d, \lfloor v_2 \rceil_d, \ldots, \lfloor v_m \rceil_d)$. A lattice in $\mathbb{Z}^m$ is a subgroup of $\mathbb{Z}^m$.

Let A be a finite set. We write $a \xleftarrow{\$} A$ to denote that a is sampled from A. We write $\mathbf{A} \xleftarrow{\$} \mathbb{Z}^{m \times n}$ to denote that every coefficients of a $m \times n$ matrix $\mathbf{A}$ are independently sampled from $\mathbb{Z}_q$. We denote the discrete Gaussian distribution over $\mathbb{Z}$ by $D_\sigma = \dfrac{\exp(x^2/(2\sigma)^2)}{1 + 2\sum_{y=1}^{\infty} \exp(y^2/(2\sigma)^2)}$. We write $\mathbf{y} \xleftarrow{\$} D_\sigma$ to denote that each coefficient of vector $\mathbf{y}$ is sampled independently from D_σ.

2.2 BG14 Signature Scheme

Next, we briefly present the signature scheme of Shi Bai and Steven Galbraith in [BG14].

Firstly, we present the public-key and secret-key generation algorithm. This algorithm, on the input of parameter set $n, m, k, q, \sigma_E, \sigma_S$ outputs a pair of matrices $(\mathbf{A}, \mathbf{T})$ as the public-key and another pair of matrices $(\mathbf{S}, \mathbf{E})$ for the secret-key.

Keygen $(n, m, k, q, \sigma_E, \sigma_S)$:	
1 :	$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$
2 :	$\mathbf{S} \xleftarrow{\$} D_S^{n\times k}$
3 :	$\mathbf{E} \xleftarrow{\$} D_E^{m\times k}$
4 :	**if** $\lvert\mathbf{E}_{i,j}\rvert > 7\sigma_E$ **then** restart at step 3
5 :	$\mathbf{T} \equiv \mathbf{AS} + \mathbf{E} \mod q$
6 :	**return** public-key $(\mathbf{A}, \mathbf{T})$ and secret-key $(\mathbf{S}, \mathbf{E})$

Figure 1: Key generation algorithm of [BG14] Signature Scheme.

Secondly, we present the signing algorithm of the signature scheme. This algorithm, on the input of the public-key $(\mathbf{A}, \mathbf{T})$, the secret-key $\mathbf{S}$, the message that one wants to sign μ, the distributions D_y, D_z, parameters w, σ_E, M, the hash function (or the random oracle) H and the encode function F that map the hash-value to the space $\mathcal{B}_{k,w}$, returns a signature $(\mathbf{z}, c)$.

Sign $(\mathbf{S}, \mathbf{A}, \mathbf{T}, \mu, D_y, D_z, d, w, \sigma_E, \mathsf{H}, \mathsf{F}, M)$:	
1 :	$\mathbf{y} \xleftarrow{\$} D_y$
2 :	$\mathbf{v} \equiv \mathbf{Ay} \mod q$
3 :	$c = \mathsf{H}(\lfloor\mathbf{v}\rceil_d, \mu)$
4 :	$\mathbf{c} = \mathsf{F}(c)$
5 :	$\mathbf{z} = \mathbf{y} + \mathbf{Sc}$
6 :	$\mathbf{w} = \mathbf{Az} - \mathbf{Tc} \mod q$
7 :	**if** $\lvert[\mathbf{w}_i]_{2^d}\rvert > 2^{d-1} - 7w\sigma_E$ **then** restart
8 :	**return** $(\mathbf{z}, c)$ with probability $\min(D_z^n(\mathbf{z})/(M \cdot D_{y,\mathbf{Sc}}^n(\mathbf{z})), 1)$

Figure 2: Signing algorithm of [BG14] Signature Scheme.

On should bare in mind that $m > n = k$ and $q > 2^d \geq B$ as the choice of parameter for the security this signature scheme.

We will not present the verify algorithm in this report. One can find it in [BG14].

3 Cryptanalyse Algorithm

Theorem 1. *Suppose that there exists an oracle which on the input a signature* $(\mathbf{z}, c)$ *returns the ephemeral key (nonce)* $\mathbf{y}$*. There exists a polynomial algorithm* *such that with n^2 signatures return the secret key $(\mathbf{S}, \mathbf{E})$ with probability $1 - 2^{-O(n)}$.*

Proof. With access to such oracle, one may easily compute $\mathbf{Sc} = \mathbf{z} - \mathbf{y}$.

From the corollary 2 in Appendix, with the probability at least $1 - 2^{-O(n)}$, there exists n linear independent vectors $\mathbf{c}_i$. Let $\mathbf{S}\mathbf{c}_i = \mathbf{r}_i$, we have:

$$\begin{bmatrix} s_{11} & s_{12} & \dots & s_{1k} \\ s_{21} & s_{22} & \dots & s_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n2} & \dots & s_{nk} \end{bmatrix} \cdot \begin{bmatrix} c_1^1 & c_2^1 & \dots & c_k^1 \\ c_1^2 & c_2^2 & \dots & c_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ c_1^k & c_2^k & \dots & c_k^k \end{bmatrix} = \begin{bmatrix} r_1^1 & r_2^1 & \dots & r_k^1 \\ r_1^2 & r_2^2 & \dots & r_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^n & r_2^n & \dots & r_k^n \end{bmatrix}$$

in which, c_i^j is the j^{th} coefficient of the vector $\mathbf{c}_i$ and similarly to r_i^j. Denote:

$$\mathbf{C} = \begin{bmatrix} c_1^1 & c_2^1 & \dots & c_k^1 \\ c_1^2 & c_2^2 & \dots & c_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ c_1^k & c_2^k & \dots & c_k^k \end{bmatrix} \qquad \mathbf{R} = \begin{bmatrix} r_1^1 & r_2^1 & \dots & r_k^1 \\ r_1^2 & r_2^2 & \dots & r_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^n & r_2^n & \dots & r_k^n \end{bmatrix}$$

We have:

$$\mathbf{SC} \equiv \mathbf{R} \mod q.$$

Since $c_1, c_2, \dots, c_n$ are linearly independent, the matrix $\mathbf{C}$ is invertible. Hence, we can easily recover:

$$\mathbf{S} \equiv \mathbf{SCC}^{-1} = \mathbf{RC}^{-1} \mod q.$$

Moreover, we have:

$$\mathbf{E} \equiv \mathbf{T} - \mathbf{AS} \mod q.$$

Therefore, there exists an efficient algorithm that with access to the mentioned above oracle, recovers the secret $(\mathbf{S}, \mathbf{E})$. □

Theorem 2. *With $O(n^3)$ signatures $(\mathbf{z}, c)$. There exists a polynomial time algorithm that recovers n vectors $\mathbf{y}_i$ correspond to the signatures $(\mathbf{z}_i, c_i)$ with non-negligible probability.*

Proof. Let's $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{n+1}$ be $n+1$ linearly dependent vectors which we are targeting with $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n$ are linear independent (remark that one can easily compute $\mathbf{c}_i$ from c_i and such set can be found with high probability thanks to corollary 2), there exists a set $a_1, a_2, \dots, a_{n+1}$ such that:

$$a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \dots + a_{n+1}\mathbf{c}_{n+1} = 0.$$

Let us denote:

$$\mathbf{p}_1 = a_1\mathbf{z}_1 + a_2\mathbf{z}_2 + \dots + a_{n+1}\mathbf{z}_{n+1},$$

we have:

$$\begin{aligned}
\mathbf{p}_1 &= a_1\mathbf{z}_1 + a_2\mathbf{z}_2 + \cdots + a_n\mathbf{z}_{n+1} \\
&= a_1(\mathbf{y}_1 + \mathbf{S}\mathbf{c}_1) + a_2(\mathbf{y}_2 + \mathbf{S}\mathbf{c}_2) + \cdots + a_n(\mathbf{y}_{n+1} + \mathbf{S}\mathbf{c}_{n+1}) \\
&= a_1\mathbf{y}_1 + a_2\mathbf{y}_2 + \cdots + a_{n+1}\mathbf{y}_{n+1} + (a_1\mathbf{S}\mathbf{c}_1 + a_2\mathbf{S}\mathbf{c}_2 + \cdots + a_{n+1}\mathbf{S}\mathbf{c}_{n+1}) \\
&= a_1\mathbf{y}_1 + a_2\mathbf{y}_2 + \cdots + a_{n+1}\mathbf{y}_{n+1} + \mathbf{S}(a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{n+1}\mathbf{c}_{n+1}) \\
&= a_1\mathbf{y}_1 + a_2\mathbf{y}_2 + \cdots + a_{n+1}\mathbf{y}_{n+1}.
\end{aligned}$$

Moreover:

$$\begin{aligned}
a_{n+1}^{-1}\mathbf{p}_1 &= a_{n+1}^{-1}a_1\mathbf{y}_1 + a_{n+1}^{-1}a_2\mathbf{y}_2 + \cdots + a_{n+1}^{-1}a_{n+1}\mathbf{y}_{n+1} + \mathbf{y}_{n+1} \\
&= a_{n+1}^{-1}a_1\mathbf{y}_1 + a_{n+1}^{-1}a_2\mathbf{y}_2 + \cdots + a_{n+1}^{-1}a_{n+1}\mathbf{y}_{n+1} + \mathbf{z}_{n+1} - \mathbf{S}\mathbf{c}_{n+1}.
\end{aligned}$$

Hence:

$$a_{n+1}^{-1}\mathbf{p}_1 - \mathbf{z}_{n+1} = a_{n+1}^{-1}a_1\mathbf{y}_1 + a_{n+1}^{-1}a_2\mathbf{y}_2 + \cdots + a_{n+1}^{-1}a_n\mathbf{y}_n - \mathbf{S}\mathbf{c}_{n+1}.$$

Let us denote $\mathbf{r}_1 = a_{n+1}^{-1}\mathbf{p}_1 - \mathbf{z}_{n+1}$, $b_i^1 = a_{n+1}^{-1}a_i$ and $\mathbf{c}'_1 = \mathbf{c}_{n+1}$ (note that $\mathbf{r}_1$ and each b_i^1 can be publicly computed) we rewrite the above equation as follow:

$$\mathbf{r}_1 = b_1^1\mathbf{y}_1 + b_2^1\mathbf{y}_2 + \cdots + b_n^1\mathbf{y}_n - \mathbf{S}\mathbf{c}'_1.$$

Furthermore, since $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ span a n dimensional vector subspace of a n dimensional vector space, we can easily find (find here can be understood as we sample another signature to get a different $\mathbf{c}$) a set of linear dependent vectors $\mathbf{c}'_i$ such that each vector $\mathbf{c}'_i$ lies in the vector space spanned by $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$. Hence, for each vector $\mathbf{c}'_i$, we have:

$$\mathbf{r}_i = b_1^i\mathbf{y}_1 + b_2^i\mathbf{y}_2 + \cdots + b_n^i\mathbf{y}_n - \mathbf{S}\mathbf{c}'_i.$$

Moreover, since these vectors $\mathbf{c}'_i$ are linearly dependent, there exists a set of $O(n)$ scalars $d_1, d_2, \ldots, d_l$ such that:

$$d_1\mathbf{c}'_1 + d_2\mathbf{c}'_2 + \cdots + d_l\mathbf{c}'_l = 0.$$

Therefore:

$$\begin{aligned}
d_1\mathbf{r}_1 + d_2\mathbf{r}_2 + \cdots + d_l\mathbf{r}_l &= \sum_{i=1}^{l} d_i\big(b_1^i\mathbf{y}_1 + b_2^i\mathbf{y}_2 + \cdots + b_n^i\mathbf{y}_n - \mathbf{S}\mathbf{c}'_i\big) \\
&= \sum_{i=1}^{l}\big(d_ib_1^i\mathbf{y}_1 + d_ib_2^i\mathbf{y}_2 + \cdots + d_ib_n^i\mathbf{y}_n - d_i\mathbf{S}\mathbf{c}'_i\big) \\
&= \sum_{i=1}^{l}\big(d_ib_1^i\big)\mathbf{y}_1 + \sum_{i=1}^{l}\big(d_ib_2^i\big)\mathbf{y}_2 + \cdots + \sum_{i=1}^{l}\big(d_ib_1^n\big)\mathbf{y}_n + \sum_{i=1}^{l}\big(d_i\mathbf{S}\mathbf{c}'_i\big) \\
&= \sum_{i=1}^{l}\big(d_ib_1^i\big)\mathbf{y}_1 + \sum_{i=1}^{l}\big(d_ib_2^i\big)\mathbf{y}_2 + \cdots + \sum_{i=1}^{l}\big(d_ib_1^n\big)\mathbf{y}_n.
\end{aligned}$$

Let us denote $b_{1,j} = \sum_{i=1}^{l} \left(d_i b_j^i\right)$ and $\mathbf{u}_1 = d_1\mathbf{r}_1 + d_2\mathbf{r}_2 + \cdots + d_l\mathbf{r}_l$ we have:

$$\mathbf{u}_1 = d_1\mathbf{r}_1 + d_2\mathbf{r}_2 + \cdots + d_l\mathbf{r}_l = b_{1,1}\mathbf{y}_1 + b_{1,2}\mathbf{y}_2 + \cdots + b_{1,n}\mathbf{y}_n,$$

Let $\mathbf{b}_1 = (b_{1,1}, b_{1,2}, \ldots, b_{1,n})$. It can be seen that $\mathbf{u}_1$ and $\mathbf{b}_1$ can be publicly computed.

Follow from lemma 3 in Appendix, with non-negligible probability, from n^2 vectors $\mathbf{b}$ sampled as above (in order to create each vector $\mathbf{b}$ as above, one requires about $O(n)$ signatures, therefore, for n^2 vectors $\mathbf{b}$, it is sufficient for one to have $O(n^3)$ signatures) , there exists n linear independent vectors $\mathbf{b}_i$. We then consider the following matrix:

$$\mathbf{B} = \begin{bmatrix} b_{1,1} & b_{1,2} & \ldots & b_{1,n} \\ b_{2,1} & b_{2,2} & \ldots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \ldots & b_{n,n} \end{bmatrix}$$

Since $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ are linear independent, $\mathbf{B}$ is an invertible matrix. Hence, the matrix $\mathbf{B}^{-1}$ exists.

Let us also denote two following matrices:

$$\mathbf{Y} = \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_n \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \\ \vdots \\ \mathbf{u}_n \end{bmatrix}$$

It is clear that:

$$\mathbf{U} = \mathbf{B}\mathbf{Y}.$$

Therefore:

$$\mathbf{Y} = \mathbf{B}^{-1}\mathbf{U}.$$

On the other hand, since $\mathbf{b}_i$ and $\mathbf{u}_i$ are publicly computed, hence $\mathbf{Y}$ can also be publicly computed. Therefore, we have an efficient algorithm to recover $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. □

Corollary 1. *With $O(n^3)$ signatures $(\mathbf{z}, c)$. There exists a polynomial time algorithm that efficiently recovers the secret key $(\mathbf{S}, \mathbf{E})$.*

Proof. From the corollary 2 in Appendix, with the probability at least $1 - 2^{-O(n)}$, there exists n linear independent vectors $\mathbf{c}_i$. Moreover, from theorem 2, one may efficiently recover the vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$. Apply the result from theorem 1, one can efficiently recover the secret key $(\mathbf{S}, \mathbf{E})$. □

References

[BG14] Shi Bai and Steven D Galbraith. An improved compression technique for signatures based on learning with errors. In *Cryptographers' Track at the RSA Conference*, pages 28–47. Springer, 2014.

4 Appendix

Lemma 1. *For every subspace H with dimension less than $k-1$, the probability that $x \notin H$ with x is sampled uniformly from $\mathcal{B}_{k,w}$ is greater than $\frac{1}{2}$.*

Proof. WLOG, suppose that H is orthogonal to the vector $(1, 1, \ldots, 1, 0, \ldots, 0)$ with the first w coefficients are 1. Let B be the event that $\mathbf{x}$ is sampled independently from $\mathcal{B}_{k,w}$ such that $\mathbf{x} \in H$, we have:

$$
\begin{aligned}
\Pr[B] &= \sum_{i=0}^{\lfloor w/2 \rfloor} \frac{\binom{w}{i}\binom{w-i}{i} 2^{w-2i} \binom{k-w}{w-2i}}{2^w \binom{w}{k}} \\
&= \sum_{i=0}^{\lfloor w/2 \rfloor} \frac{\frac{w!}{(i!)^2 (w-2i)!} \frac{1}{2^{2i}} \binom{k-w}{w-2i}}{\binom{w}{k}} \\
&= \sum_{i=0}^{\lfloor w/2 \rfloor} \frac{\frac{w!}{(2^i i!)^2 (w-2i)!} \binom{k-w}{w-2i}}{\binom{w}{k}} \\
&\leq \sum_{i=0}^{\lfloor w/2 \rfloor} \frac{\frac{w!}{2(2i)!(w-2i)!} \binom{k-w}{w-2i}}{\binom{w}{k}} \\
&= \frac{1}{2} \sum_{i=0}^{\lfloor w/2 \rfloor} \frac{\binom{w}{2i}\binom{w-k}{w-2i}}{\binom{w}{k}} \\
&< \frac{1}{2}.
\end{aligned}
$$

Hence, the probability that $\mathbf{x} \notin H$ is greater than $\frac{1}{2}$. □

Corollary 2. *The probability that a set of k^2 vectors sampled independently from $\mathcal{B}_{k,w}$ contain no k linear independent vectors is exponentially small.*

Proof. Let $\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_{k^2}$ be k^2 vectors chosen independently form $\mathcal{B}_{k,w}$. For $i = 1, 2, \ldots, k$ let B_i be the event that:

$$\dim \operatorname{span}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{(i-1)k}) = \dim \operatorname{span}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{ik}) < k.$$

If none of the event B_i happens, then $\dim \operatorname{span}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k^2}) = k$. Hence, to complete the proof, we only need to show that, for every i then $\Pr[B_i] \leq 2^{-O(n)}$. With some fixed i, let us condition on some fixed choice of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{(i-1)k}$ such that $\dim span(\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_{(i-1)k}) < k$. From lemma 1, The probability that:

$$\mathbf{x}_{(i-1)k+1}, \mathbf{x}_{(i-1)k+2}, \ldots, \mathbf{x}_{ik} \in \operatorname{span}(\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_{(i-1)k})$$

is less than $(1/2)^k = 2^{-O(k)}$. Moreover, since $k = n$, the probability that each B_i happens is $2^{-O(n)}$. □

Lemma 2. *Let D be a distribution such that for every subspace H with dimension less than $n-1$, the probability that $x \notin H$ with x is sampled from D is greater than $\frac{1}{2}$. For every fixed positive number l, let us sample $a_1, a_2, \ldots, a_m$ from an uniform distribution over $\mathbb{Z}_q^n$ and $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_l$ from D. Let D' be the distribution of $x = \sum_{i=1}^{l} a_i x_i$ then for every subspace H with dimension less than $n-1$, the probability that $x \notin H$ with x is sampled from D' is also greater than $\frac{1}{2}$.*

Proof. WLOG, let us fixed a subspace H with dimension $n-1$. For every $1 \leq i \leq l$, let $\mathbf{x}_i = \mathbf{x}'_i + \mathbf{h}_i$ with $\mathbf{h}_i \in H$ and $\mathbf{x}'_i \in H^{\perp}$. Since the probability that $x \notin H$ with x is sampled from D is greater than $\frac{1}{2}$, there exists at least one $\mathbf{x}'_i$ such that $\mathbf{x}'_i \neq 0$ with probability $1 - 2^{-l}$. We have:

$$\begin{aligned}
&\Pr[(a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \cdots + a_l\mathbf{x}_l) \in H] \\
=&\Pr[\big(a_1(\mathbf{x}'_1 + \mathbf{h}_1) + a_2(\mathbf{x}'_2 + \mathbf{h}_2) + \cdots + a_l(\mathbf{x}_l + \mathbf{h}_l)\big) \in H] \\
=&\Pr[\big(a_1\mathbf{x}'_1 + a_2\mathbf{x}'_2 + \cdots + a_l\mathbf{x}'_l\big) \in H] \\
=&\Pr[\big(a_1\mathbf{x}'_1 + a_2\mathbf{x}'_2 + \cdots + a_l\mathbf{x}'_l\big) = 0] = \frac{1}{q} \\
\leq&\frac{1}{2}.
\end{aligned}$$

Therefore, the probability that $x \notin H$ with x is sampled uniformly from D' is greater than $\frac{1}{2}$. □

Lemma 3. *The probability that a set of n^2 vectors sampled independently from the distribution of the vectors $\mathbf{b}$ contain no n linear independent vectors is exponentially small.*

Proof. For the sake of simplicity, let us fix $l = n+1$. Consider the distribution of the vectors $(b_1^i, b_2^i, \ldots, b_n^i)$, we have:

$$b_1^i\mathbf{c}_1 + b_2\mathbf{c}_2^i + \cdots + b_n^i\mathbf{c}_n = \mathbf{c}'_i.$$

It is clear that $(b^i_1, b^i_2, \ldots, b^i_n)$ is the representation of vector $\mathbf{c}'_i$ in the basis $\big(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n\big)$. Hence, if the set of vectors $\mathbf{c}'_1, \mathbf{c}'_2, \ldots, \mathbf{c}'_l$ is linearly independent then the set of vectors $\{(b^i_1, b^i_2, \ldots, b^i_n)\}_{i=1}^{l}$ is also linearly independent and vice versa. Therefore, the distribution of the vectors $(b^i_1, b^i_2, \ldots, b^i_n)$ also satisfy the property that for every subspace H with dimension less than $n-1$, the probability that $x \notin H$ with x is sampled this distribution is greater than $\frac{1}{2}$. Moreover, since the distribution of $\{(b^i_1, b^i_2, \ldots, b^i_n)\}_{i=1}^{l}$ and the set of scalars $\{d_1, d_2, \ldots, d_l\}$ are independent, applying the result from lemma 2, the probability that $\mathbf{b} \notin H$ is also greater than $\frac{1}{2}$.

Using the same argument as in corollary 2, one can conclude that the probability that a set of n^2 vectors sampled independently from the distribution of the vectors $\mathbf{b}$ contain no n linear independent vectors is $2^{-O(n)}$.

$\square$