

# A generalization of a reconciliation mechanism

August 19, 2015

Here we focus on the even modulus, for simplicity we will assume that the modulus is a power of two (in our instantiation/implementation  $q = 2^{32}$ ).

In the Section 1 we describe the mechanism for extracting 2 bits ([Pei14] describes the mechanism for extracting 1 bit) from a single ring element. In Section 2 we generalize the mechanism to extracting an arbitrary number of bits (as long as the noise is not too big). In Section 3 we show how these changes affect the correctness of key exchange by upper bounding the probability for two parties to get different keys.

## 1 Extracting 2 bits from a single element

Following the original idea of Peikert [Pei14] for element  $v \in \mathbb{Z}_q$  we define functions

$$\begin{aligned} \lfloor \cdot \rfloor_4 : \mathbb{Z}_q &\rightarrow \{0, 1, 2, 3\} \text{ s.t. } \lfloor v \rfloor_4 = \left\lfloor \frac{4}{q} v \right\rfloor \\ \langle \cdot \rangle_4 : \mathbb{Z}_q &\rightarrow \{0, 1\} \text{ s.t. } \langle v \rangle_4 = \left\lfloor \frac{8}{q} v \right\rfloor \bmod 2 \end{aligned}$$

We define disjoint intervals  $I_0 := \{0, 1, \dots, \frac{q}{4} - 1\}$ ;  $I_k := I_0 + k \cdot \frac{q}{4}$ , where  $k \in \{1, 2, 3\}$ .

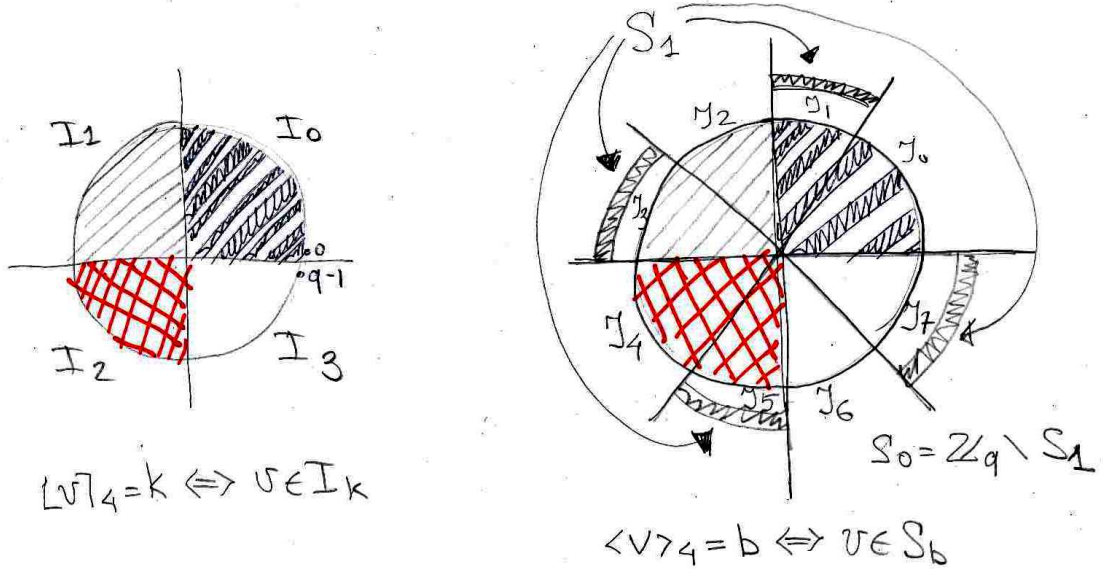
$$\lfloor v \rfloor_4 = k \text{ iff } v \in I_k.$$

We define disjoint intervals which are twice smaller:  $J_0 := \{0, 1, \dots, \frac{q}{8} - 1\}$ ;  $J_k := J_0 + k \cdot \frac{q}{8}$ , where  $k \in \{1, \dots, 7\}$ .

Lets define  $S_0 = J_0 \cup J_2 \cup J_4 \cup J_6$ , and  $S_1 = J_1 \cup J_3 \cup J_5 \cup J_7 = \mathbb{Z}_q \setminus S_0$ .

$$\langle v \rangle_4 = b \text{ iff } v \in S_b,$$

The partition is shown on the picture below:



**Claim 1.** If  $v \in \mathbb{Z}_q$  is uniformly random, then  $[v]_4$  is uniformly random given  $\langle v \rangle_4$ .

*Proof.* For any  $b \in \{0, 1\}$ , if we condition on  $\langle v \rangle_4 = b$ , then  $v$  is uniform over  $J_b \cup J_{2+b} \cup J_{4+b} \cup J_{6+b}$ . If  $v \in J_{b+2k}$ , then  $[v]_4 = k$ , so  $[v]_4$  is uniformly random given  $\langle v \rangle_4$ .  $\square$

Define the reconciliation function  $rec : \mathbb{Z}_q \times \{0, 1\} \rightarrow \mathbb{Z}_4$  as

$$rec(w, b) := k \text{ if } w \in J_{2k+b} + E$$

**Claim 2.** If  $w = v + e \pmod q$  for  $v \in \mathbb{Z}_q$  and  $e \in E$ , where  $E = \left[-\frac{q}{16}, \frac{q}{16}\right) \cap \mathbb{Z}$ , then  $rec(w, \langle v \rangle_4) = [v]_4$

*Proof.* Let  $b = \langle v \rangle_4 \in \{0, 1\}$ , so  $v \in J_b \cup J_{2+b} \cup J_{4+b} \cup J_{6+b}$ . Then  $[v]_4 = k$  if and only if  $v \in I_k$ . This holds if and only if  $w \in J_{2k+b} + E$ , because  $J_{2k+b} + E$  are disjoint for different  $k$ 's.  $\square$

## 2 Extracting $B$ bits from a single element

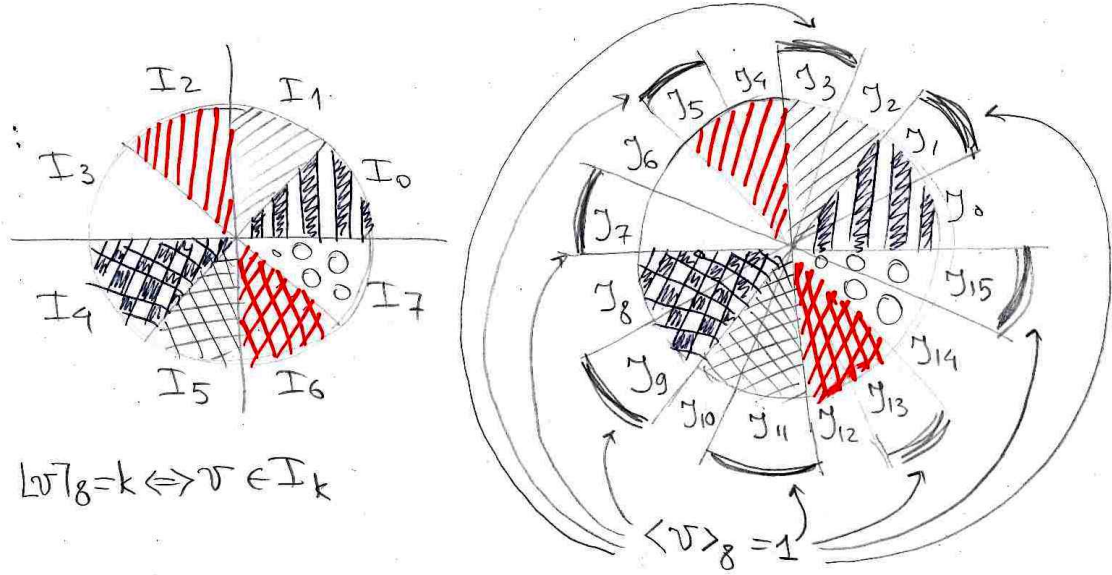
The approach described above can be generalized to extracting  $B$  bits. We again define functions

$$\begin{aligned} [\cdot]_{2^B} : \mathbb{Z}_q &\rightarrow \{0, \dots, 2^B - 1\} \text{ s.t. } [v]_{2^B} = \left\lfloor \frac{2^B}{q} v \right\rfloor \\ \langle \cdot \rangle_{2^B} : \mathbb{Z}_q &\rightarrow \{0, 1\} \text{ s.t. } \langle v \rangle_{2^B} = \left\lfloor \frac{2^{B+1}}{q} v \right\rfloor \pmod 2 \end{aligned}$$

We again define  $2^B$  intervals  $\{I_k\}$  and  $2^{B+1}$  intervals  $\{J_{2k+b}\}$  such that

$$\begin{aligned} [v]_4 &= k \text{ iff } v \in I_k, \\ \langle v \rangle_4 &= b \text{ iff } v \in J_{b+2k} \text{ for some } k. \end{aligned}$$

The case of  $B = 3$  is shown on the picture below:



Similar claims can be proven for  $E = [-\frac{q}{2^{B+2}}, \frac{q}{2^{B+2}}) \cap \mathbb{Z}$ .

### 3 Correctness for key exchange mechanism

For correctness we require that for all pairs of indices  $(i, j)$ ,  $|(E'S + S'E + E'')_{ij}| < \frac{q}{2^{2+B}} - \frac{1}{2}$ . Here  $S, E \in \mathbb{Z}_q^{n \times \bar{n}}$ ,  $S', E' \in \mathbb{Z}_q^{\bar{m} \times n}$ ,  $E'' \in \mathbb{Z}_q^{\bar{m} \times \bar{n}}$  and they all are draw from a Gaussian distribution with standard deviation  $\sigma$ . For a fixed pair  $(i, j)$ , we bound the probability of  $|(E'S + S'E + E'')_{ij}| > \frac{q}{2^{2+B}} - \frac{1}{2}$  as follows. There are  $2n + 1$  terms in the sum, if the  $(ij)$  element is greater than  $\frac{q}{2^{2+B}} - \frac{1}{2}$ , then at least one of the elements of the gaussian matrix must exceed  $z = \sqrt{\frac{q}{2^{2+B}(2n+1)}}$  in absolute value. The probability of individual gaussian coefficient exceeding  $z$  in absolute value can be bounded by  $e^{-(z/(\sqrt{2}\sigma))^2}$ . The probability that one out of  $(4n + 1)$  exceeds  $z$  is bounded above by the sum  $(4n + 1)e^{-(z/(\sqrt{2}\sigma))^2}$ . Similarly, the probability that at least one coefficient of  $k_A$  and  $k_B$  disagree is clearly bounded above by the sum of all the  $p_{ij}$ , so we get

$$\Pr(k_A \neq k_B) \leq \sum_{i=0}^{\bar{n}} \sum_{j=0}^{\bar{n}} p_{ij} \leq \bar{n} \cdot \bar{m} (4n + 1) e^{-q/(2 \cdot 2^{2+B} (2n+1) \sigma^2)} \quad (1)$$

For our choice of parameters:  $q = 2^{32}$ ,  $n = 1024$ ,  $\bar{n} \cdot \bar{m} = 128$ ,  $\sigma = 3.2$ , for different numbers of extracted bits the decay in this probability is shown in the table below:

$$\begin{aligned} (\bar{n} \cdot \bar{m})(4n + 1) e^{-q/(2 \cdot 2^{2+B} (2n+1) \sigma^2)} &= \\ 2^7 \cdot 2^{12} \exp\left(-\frac{2^{32}}{2^{3+B} \cdot 2^{11} \cdot \sigma^2}\right) &= \\ 2^{19} \exp(-2^{18-B}/\sigma^2) &= \\ 10^{\log_{10} 2 \cdot 19 - \log_{10} e \cdot 2^{18-B}/\sigma^2} \end{aligned}$$

Bits extracted from one ring element ( $i$ )	Probability of failure
1	1e-5553
2	1e-2773
3	1e-1384
4	1e-689
5	1e-341
6	1e-167
7	1e-81
8	1e-37
9	1e-15
10	1e-5
11	1e1

Note: 1e-x stands for  $10^{-x}$ .

The parameters of the scheme scale as  $\frac{1}{\sqrt{B}}$ .

## References

- [Pei14] Chris Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography*, pages 197–219. Springer, 2014.