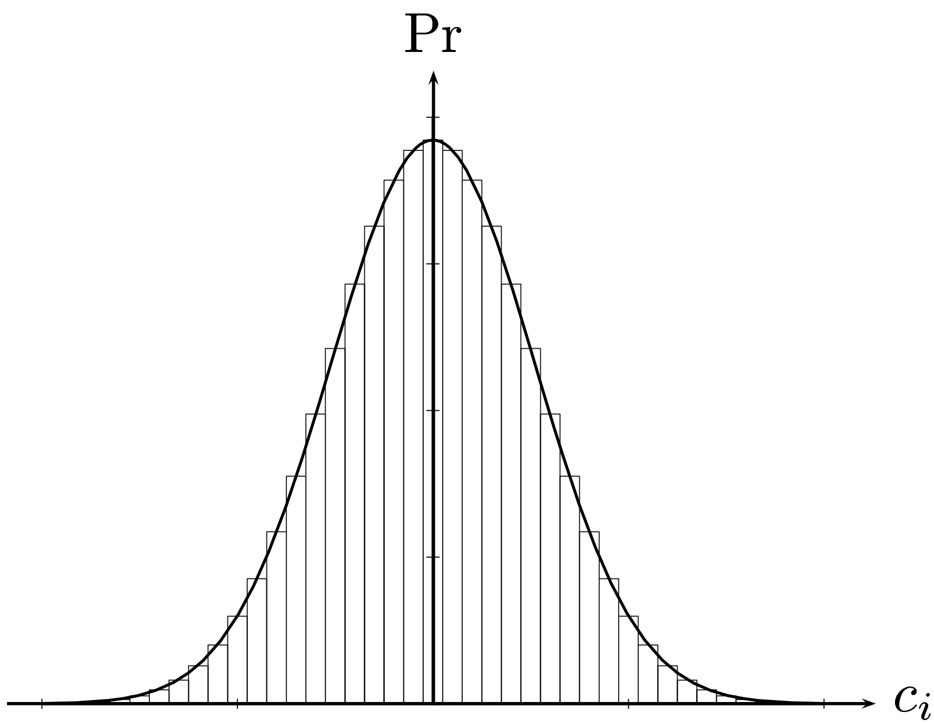
Convolution Rings and Related Cryptographic Schemes

Sven Laur
swen@math.ut.ee

University of Tartu



Introduction. Motivation

- The common public-key cryptosystems are slow because they usually involve exponentiation.

- Reasonable crypto schemes use addition $+$ and substraction $-$, multiplication $\star$ and invertibility.

- Polynomial ring $\mathbb{Z}[X]$ possesses efficient $+$, $-$, $\star$ and but lacks $\square^{-1}$.

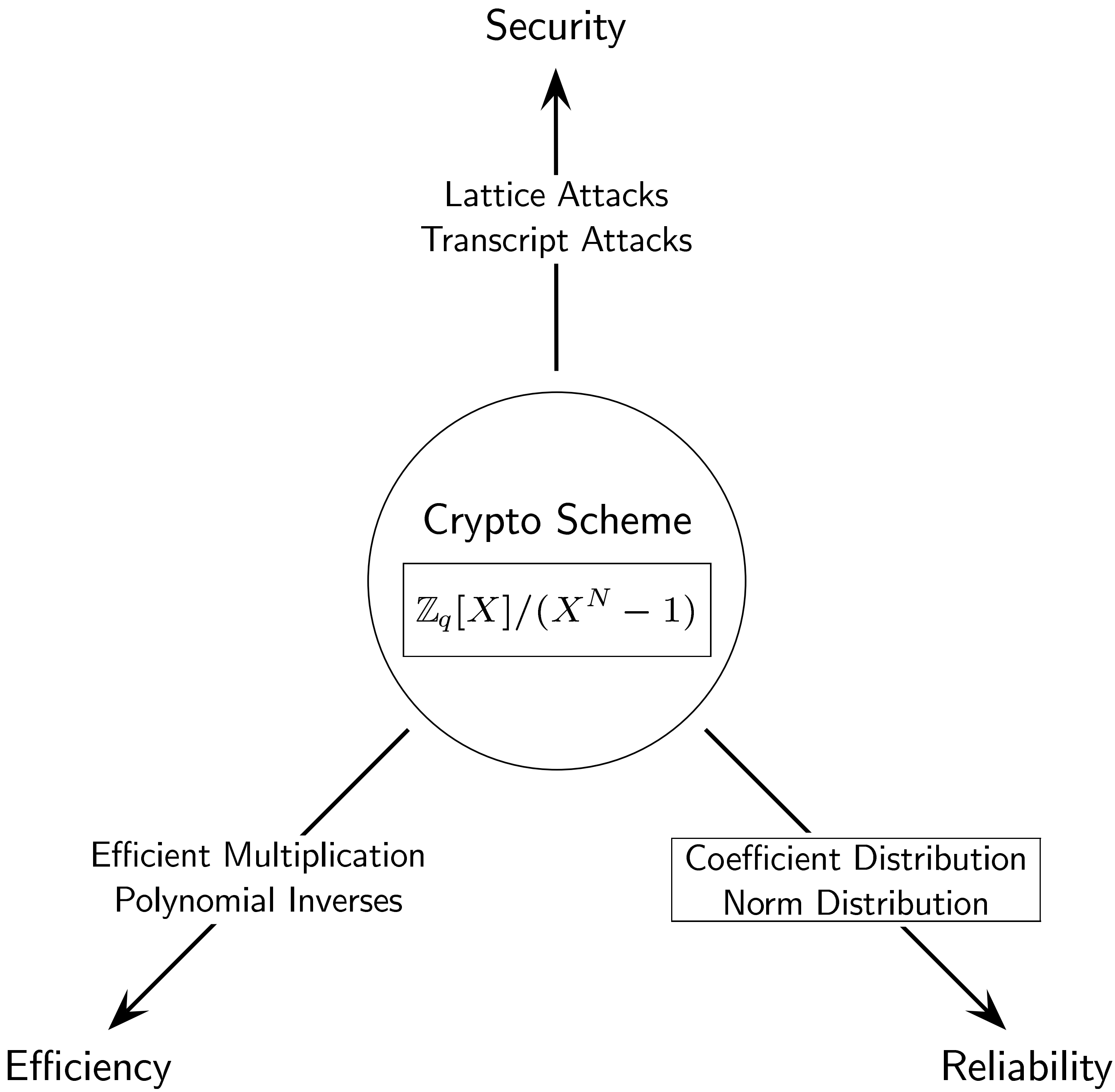
- The multiplication rule in $\mathbb{Z}_q[X]/(X^N - 1)$ is very simple. If $h = f \circledast_q g$ then

$$h_k \equiv \sum_{i+j \equiv k \mod N} f_i g_j \mod q$$

- Factor ring $\mathbb{Z}_q[X]/(X^N - 1)$ has the same properties as $\mathbb{Z}[X]$ and many polynomials f have inverses F_q such that $f \circledast_q F_q = 1$.

- If $q = 2^k$ then there is a simple and natural way to implement $\mathbb{Z}_q[X]/(X^N - 1)$.

Related Cryptographic Shemes



Encyption scheme NTRU

NTRU uses double reduction modulo q and modulo p. The integers p and q must be relatively prime.

Key generation

$$h \overset{q}{\leftarrow} F_q \circledast g \qquad\qquad \begin{aligned} f &\in \mathcal{L}(d_f, d_f - 1) \\ g &\in \mathcal{L}(d_g, d_g) \end{aligned}$$

Encryption

$$e \overset{q}{\leftarrow} p\phi \circledast h + m \qquad\qquad \phi \in \mathcal{L}(d_\phi, d_\phi)$$

Decryption

$$a \overset{q}{\leftarrow} f \circledast e$$

$$m \overset{p}{\leftarrow} F_p \circledast a$$

Simple decryption criterion

$$\left\| p\phi \circledast g + f \circledast m \right\|_\infty < \frac{q}{2}$$

$$\left| p \cdot \mathrm{coeff}\left(\phi \circledast g, i\right) + \mathrm{coeff}\left(f \circledast m, i\right) \right| < \frac{q}{2}$$

Coefficient distributions

Due to multiplication rule the coefficients of $c = f \circledast m$ have identical distributions

$$c_i = \sum_{i=1}^{d_1+d_2} X_i, \text{ where } X_i \underset{u}{\leftarrow} \{-1, 0, 1\}$$

It can be computed exactly

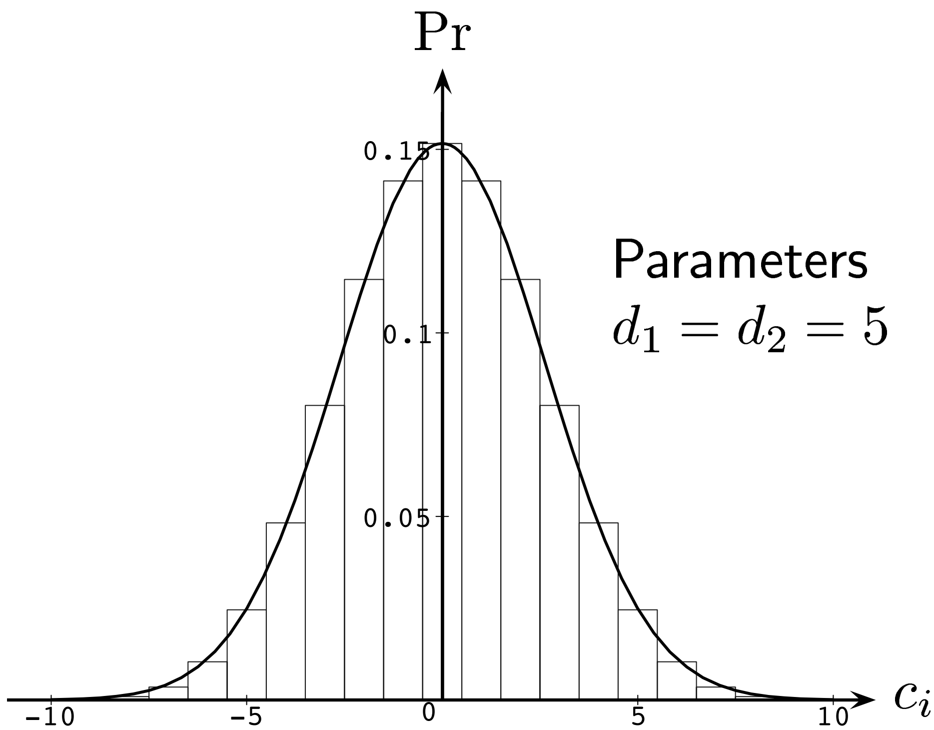
$$\Pr\left[c_i = C\right] = \frac{1}{3^{d_1+d_2}} \sum_{k=0}^{d_1+d_2} \binom{d_1+d_2}{k} \binom{d_1+d_2-k}{k-C}$$

but this is time consuming and the result is too exact. Berry-Esséen theorem promises convergence to normal distribution $\mathcal{N}(0, \sigma)$. Practical experiments suggest that convergence is rapid. We find σ indirectly

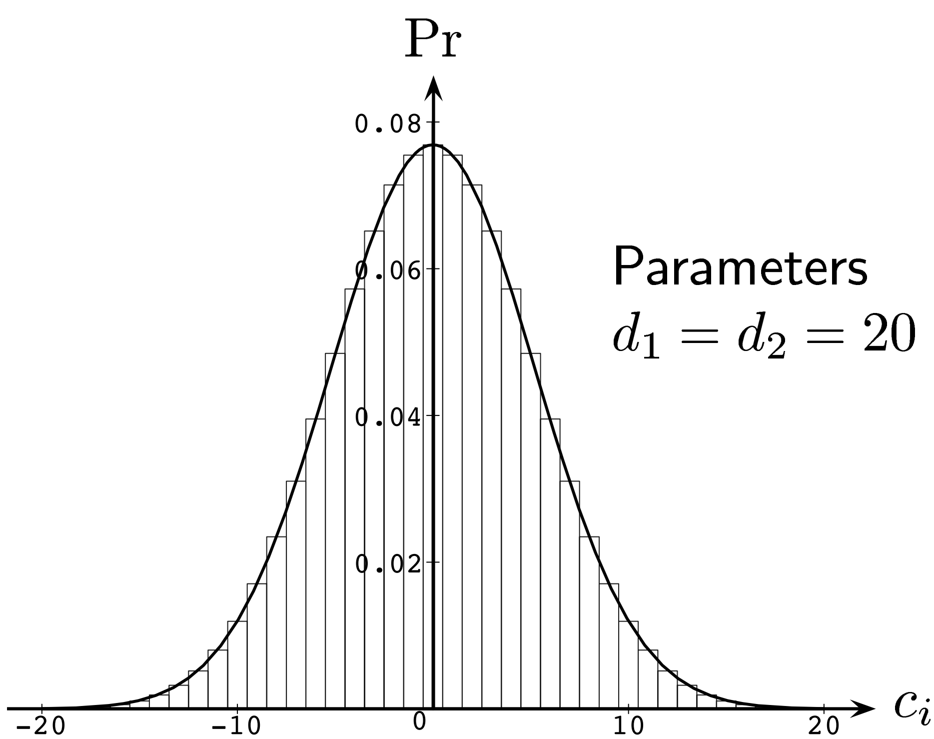
$$\sigma = \frac{1}{\sqrt{2\pi} \Pr\left[\text{coeff}\left(f \circledast m\right) = 0\right]}$$

This methodology can be used to calculate $\phi \circledast g$. This distribution can also be approximated with normal distribution although here we have weak correlation between X_i.

Approximation examples



Parameters
$d_1 = d_2 = 5$



Parameters
$d_1 = d_2 = 20$

Further enhancements

How to approximate the distribution?

$$p \cdot \mathrm{coeff}\,(\phi \circledast g, i) + \mathrm{coeff}\,(f \circledast m, i)$$

If two random variables $X_1 \sim \mathcal{N}(\mu_1, \sigma_1)$ and $X_2 \sim \mathcal{N}(\mu_2, \sigma_2)$ are independent then

$$X_1 + X_2 \sim \mathcal{N}\Big(\mu_1 + \mu_2, \sqrt{\sigma_1^2 + \sigma_2^2}\,\Big).$$

We have constraint $2 < p$ because the $\gcd(p, q) = 1$! The integer p disperses the summary distribution. Solution p can be a polynomial! What is the distribution of $S = p \circledast \phi \circledast g$?

$$S_i = \sum_{k=1}^{r} p_k X_k \qquad X_k \sim \mathcal{N}(\mu, \sigma)$$

So we know that

$$\mu_S = \mu \sum_{k=1}^{r} p_k \qquad \sigma_S = \|p\|_2 \sigma$$

The best known candidates $p = X \pm 2$ have identical norms $\|X \pm 2\| = \sqrt{5} \approx 2.24$ so from probabilistic viewpoint there is no difference.

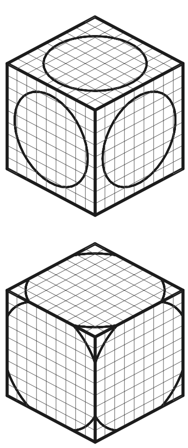
NTRUSIGN and norm distributions

NTRUSIGN is a more efficient simplification of Goldreich-Goldwasser-Halevi signing scheme. The reliability of NTRUSIGN depends on centered norm distributions of $f \circledast m$ which can be approximated with χ^2-distribution. The aproximation can be determined by the mathematical expectation μ and standard deviation σ which can be calculated.

The security of NTRUSIGN depends on norm distribution

$$W = \sum_{i=0}^{N-1} X_i^2 \qquad\qquad X_i \underset{u}{\leftarrow} \left[-\frac{1}{2}, \frac{1}{2}\right]$$

This converges quickly to normal distribution but the convergence is not quick enough to give security proofs.



The corresponding problem has a simple geometric interpretation – probability is the volume of intersection of unit cube and ball in N-dimendional space. But the direct computation of the volume is Herculean task due to complex geometric structure of intersection.

Experimental norm distributions