EXAME Criptografia e Segurança da Informação — DURAÇÃO 2:30
CURSO MEI — 19·Janeiro·2015

I

Existe um relação estreita entre códigos Reed-Solomon e o designado "problema da reconstrução polinomial com ruído" (NPR).

1. Descreva o problema e discuta as circunstâncias em que é criptograficamente "difícil".
2. Como é que a solução de NPR é usada nos códigos Reed-Solomon?
3. Como é possível transformar o criptosistema de McElice de modo a usar códigos de Reed-Solomon em vez de códigos de Goppa?

II

Curvas elípticas determinam grupos cíclicos criptograficamente relevantes que são uma alternativa aos grupos multiplicativos de inteiros usados na versão original do "Digital Signature Algorithm" (FIPS 186-1, 1994).

1. Descreva de que forma se constroem os grupos cíclicos de uma e de outra forma.
2. Que vantagens e desvantagens existem na utilização de um e outro tipo de grupo cíclico.
3. Os grupos em curvas elípticas permitem, adicionalmente, construir "emparelhamentos". Defina emparelhamentos e dê um exemplo da sua relevância criptográfica.

III

Basear uma técnica criptográfica em problemas que, no caso geral, são difíceis apenas "no pior caso", não dá suficiente confiança à sua segurança. É mais seguro basear a técnico num problema que é difícil "no caso médio", ou, ainda melhor, "no melhor caso".

1. No pior caso, a complexidade do problema da factorização de inteiros não é superior à complexidade do "closest vector problem" (CVP) em reticulados. Justifique esta afirmação.
2. É possível relacionar o pior caso e o caso médio do "shortest vector problem"; descreva a relação que existe entre estes problemas.
3. O "pigeon hole principle" (PHP) permite definir situações onde a complexidade de exprime no "melhor caso". Defina o problema e indique a sua complexidade.

IV

Recentemente recorre-se a uma combinação da teoria dos ideais, com reticulados e problemas de aprendizagem, para construir novos criptosistemas com garantias adicionais de segurança mas também com novas funcionalidades. Nesta categoria destaca-se a utilização de ideias em anéis de polinómios no problema "Learning With Errors" (LWE) e nos criptosistemas homomórficos.

1. Como se define o problema "LWE" que usam reticulados sobre anéis de polinómios? Defina o problema, discuta a sua complexidade e a sua relação com o "shortest vector problem".
2. Que propriedades deve verificar uma cifra para ser considerada "completamente" homomórfica? Apresente a definição genérica de uma cifra que verifique estas propriedades?
3. Que razão levam à implementação da cifra homomórfica de Gentry sobre reticulados de polinómios?