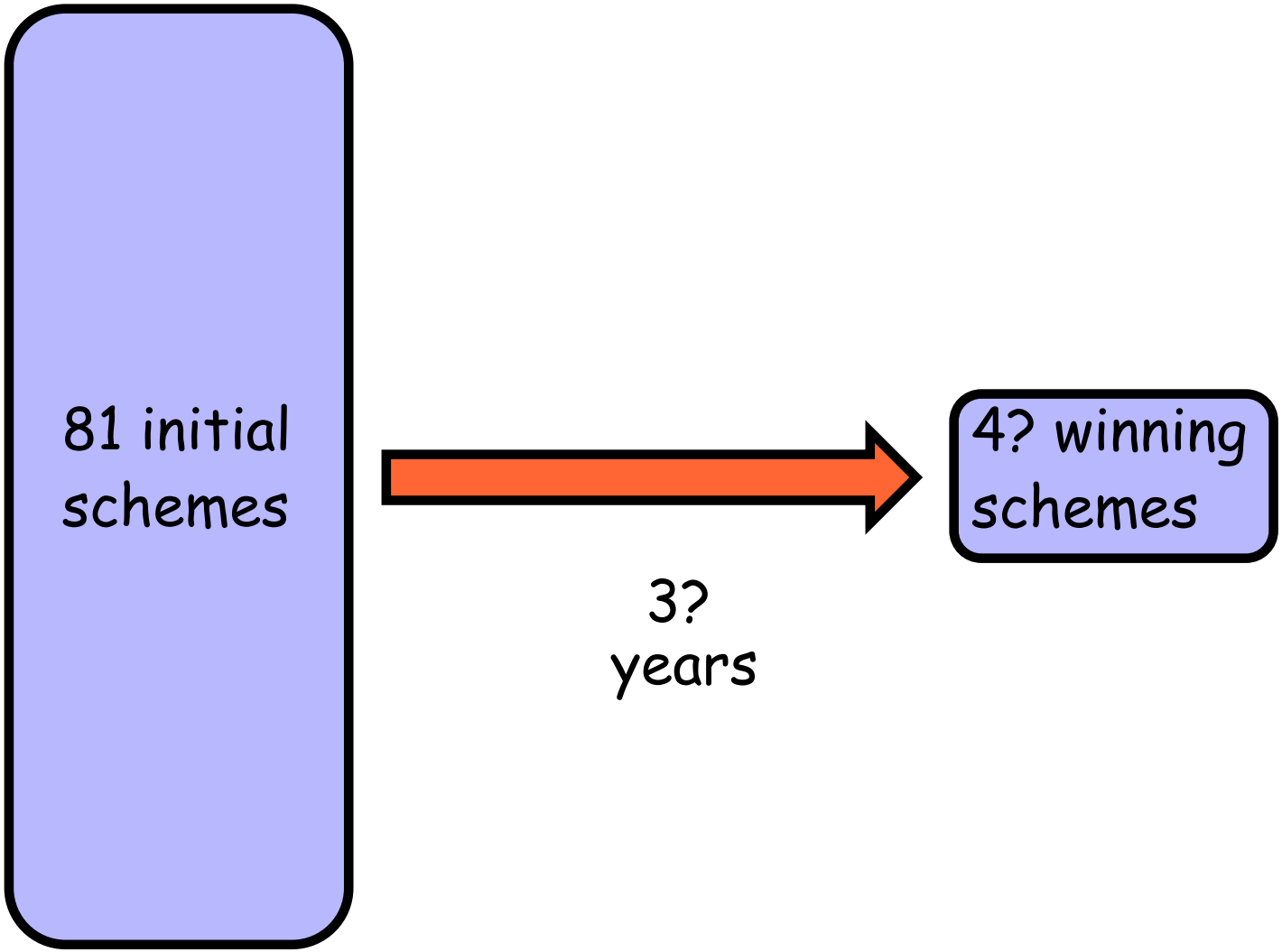
PQ-Crypto:
A New Proposed Framework

Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel

The Proposed NIST Framework:



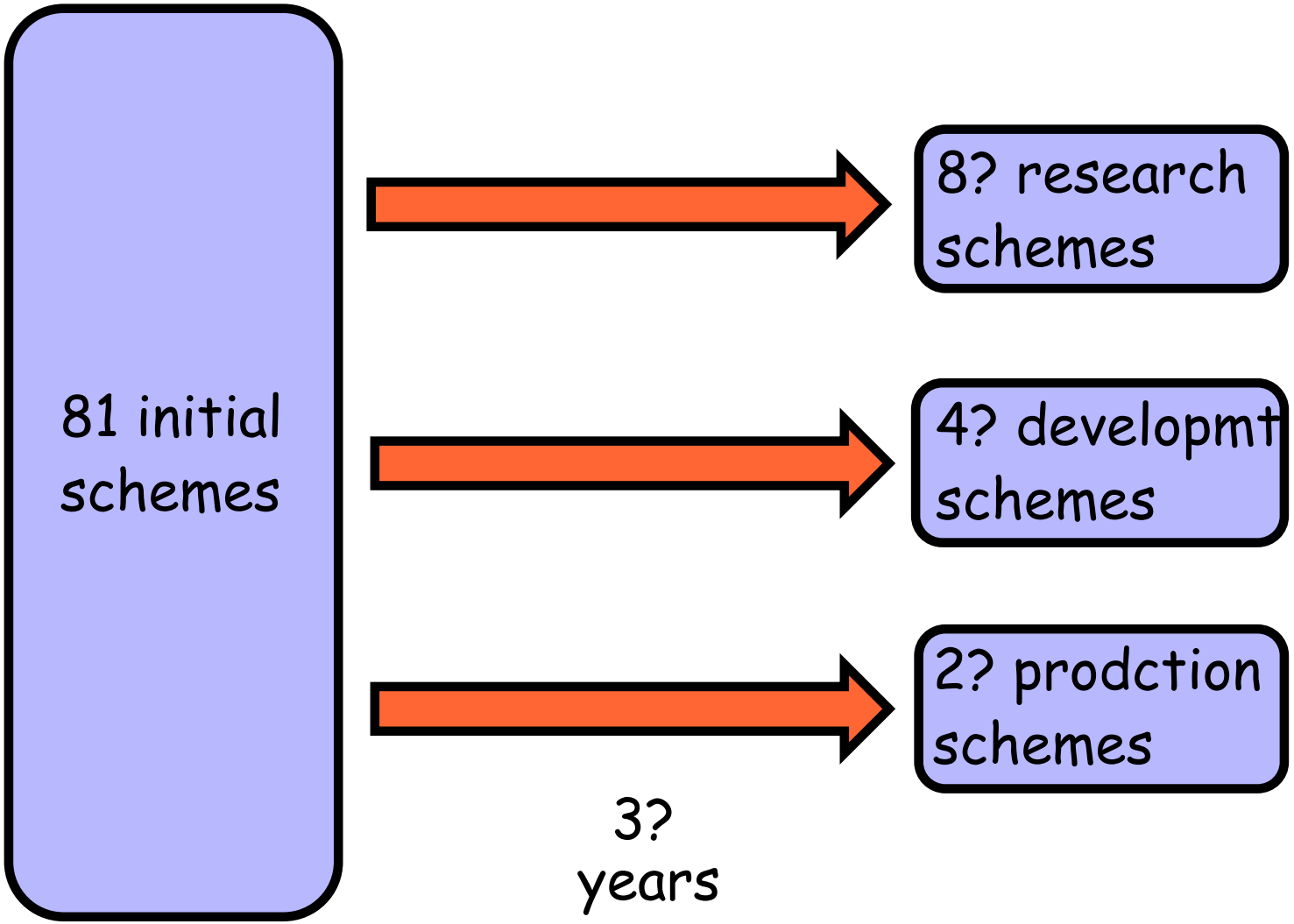
Problems with this Framework:

- The winning schemes should have conflicting properties: They should have good performance, be highly trusted, and be ready for immediate deployment. However:
- Developing new PKC is harder and riskier than SKC
- Many "infant mortalities" are expected for new ideas
- There is no immediate need to widely deploy a winner

Most companies create new products by going through three distinct phases:

- Research: Studying brand new ideas, science based
- Development: Fine-tuning, engineering based
- Production: Large-scale manufacturing, factory based

I Propose to Use this RDP Framework:



The Production Schemes:

- These are the schemes that NIST recommends for actual wide-scale deployment by the industry
- It can remain empty until there is a real imminent threat from quantum computers
- The production schemes will be typically chosen from the development list

The Development Schemes:

- The main criteria for inclusion in this list will be TTT: Time-Tested / Trusted
- Schemes in this list should have at least 15 years of analysis behind them
- Initial choices can include a basic lattice scheme, the McEliece scheme, NTRU, but not schemes based on isogeny or Mersenne
- Companies should program and study them

The Research Schemes:

- The main criteria for inclusion in this list will be PPP: Promising Properties / Performance
- These will NOT be schemes that NIST recommends for actual production, and thus this list can contain some high risk candidates
- The goal of the research list is just to concentrate the effort of the research community on fewer candidate schemes