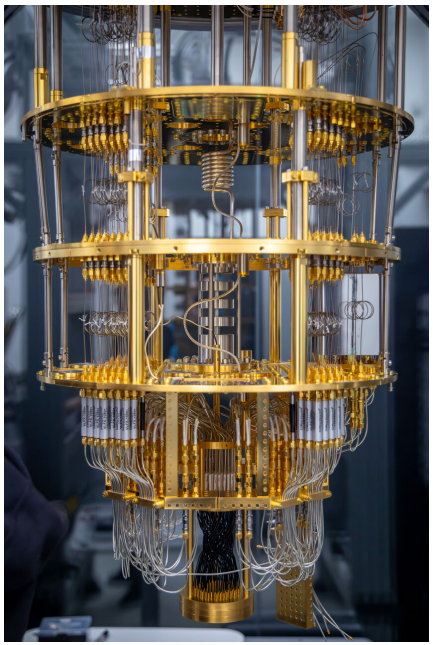
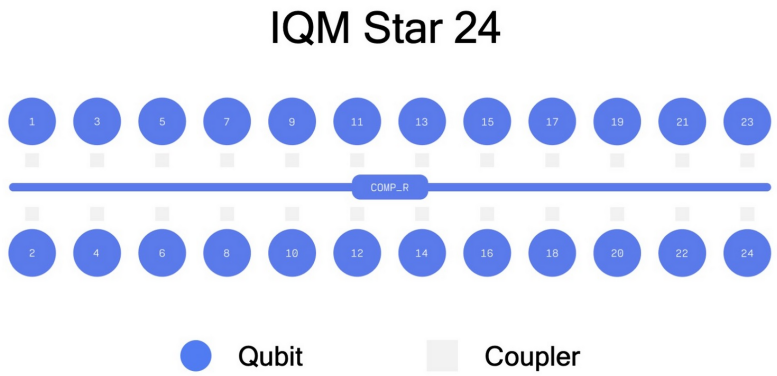
Noise resilient Quantum Key Distribution

Ryszard Kukulski



VSB TECHNICAL UNIVERSITY OF OSTRAVA | IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER



Outline

What we will talk about:

- QKD framework,
- Safety and reliability concerns,
- Noise models and Eve modeling,
- Optimality of QKD methods.

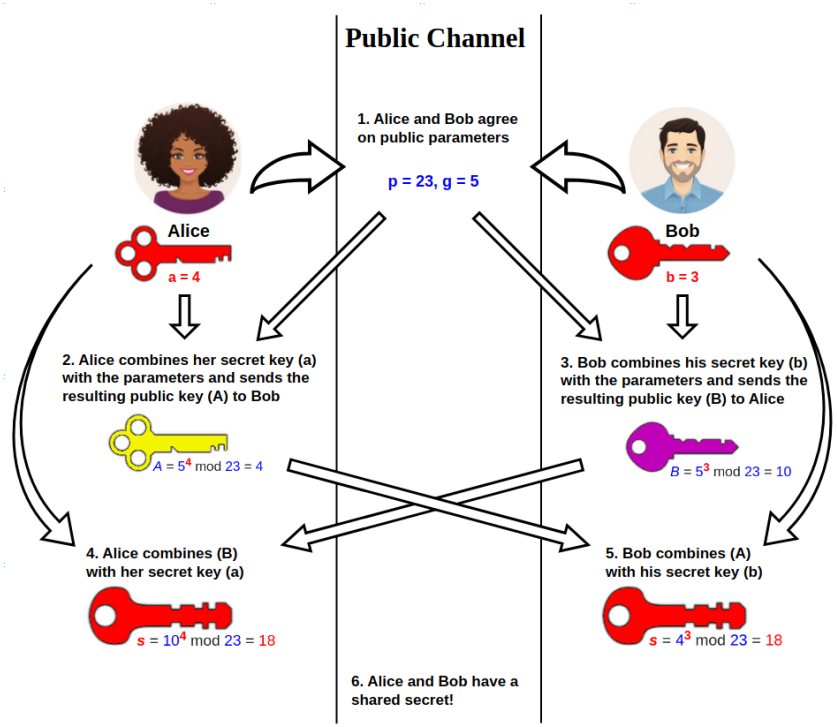
What we will not talk about:

- Classical post-processing (in details),
- Transmission lines and technology,
- Photon Number Splitting attack and decoy states,
- Side-channels,
- ...

Key Distribution without Quantum

Exemplary key distribution methods:

- Diffie–Hellman key exchange,
- RSA cryptosystem,
- Elliptic-curve cryptography,
- Lattice-based cryptography (post-quantum)



Wikipedia

How it started: BB84 (Charles Bennett and Gilles Brassard)

Alice states:

- $|0\rangle$ as key '0' in Z basis,
- $|1\rangle$ as key '1' in Z basis,
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ as key '0' in X basis,
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as key '1' in X basis.

Bob measurement:

- Z basis $(|0\rangle, |1\rangle)$,
- X basis $(|+\rangle, |-\rangle)$.

A / B	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$1/8$	0	$1/16$	$1/16$
$\|1\rangle$	0	$1/8$	$1/16$	$1/16$
$\|+\rangle$	$1/16$	$1/16$	$1/8$	0
$\|-\rangle$	$1/16$	$1/16$	0	$1/8$

Figure: Probability distribution table

BB84 - Eve attacks

Attack 1

Eve grabs transmitted state, measures it Z basis and sends Bob the measured state.

$P(K_A = K_B|S) = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$

$P(K_A = K_E|S) = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$

BB84 - Eve attacks

Attack 2

Eve grabs transmitted state, sends Bob state $|0\rangle$ and measures collected state in the announced basis.

$P(K_A = K_B|S) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$

$P(K_A = K_E|S) = 1$

QKD - quantum framework

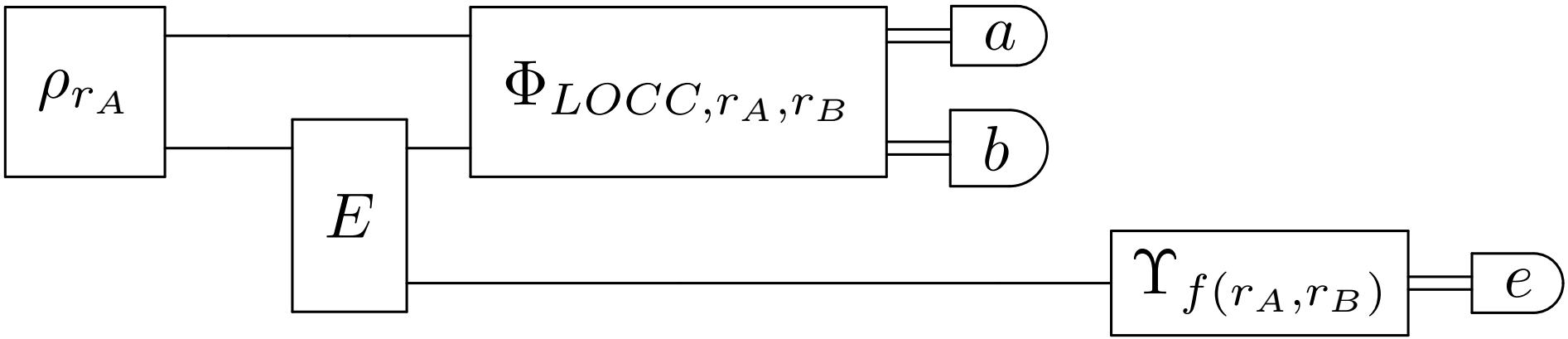


Figure: General quantum framework where Alice and Bob conduct series of independent experiments. Each of them, contains single qubit transmission and communication through authenticated classical channel (conditions following: Sandfuchs, Martin, et al. "Security of differential phase shift QKD from relativistic principles." Quantum 9 (2025): 1611.)

QKD - quantum framework

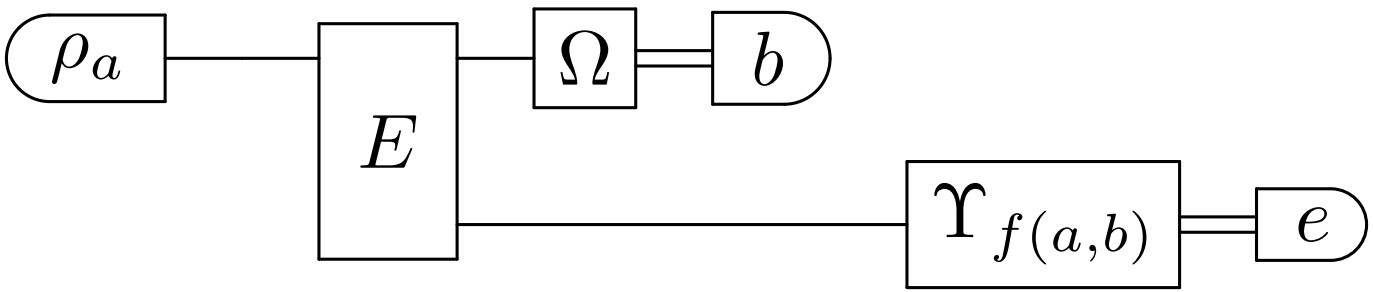


Figure: Equivalent standardized quantum framework

QKD - classical framework

Theorem

For a sequence of independent experiments, the achievable key ratio can be bounded by

$$S(A;B||E) \geq I(A;B) - I(A;E) \tag{1}$$

Csiszár, Imre, and Janos Korner. "Broadcast channels with confidential messages." IEEE transactions on information theory 24.3 (2003): 339-348.

Full procedure overview

Definition of the protocol components:

1. QKD-1q: p_a, ρ_a, Ω.
2. Acceptable ratio x, that is $P_E(K_A = K_B|S) \geq x$.
3. Error correction and Privacy amplification methods.

Protocol:

1. Making X_1 independent quantum experiments.
2. X_2 of X_1 experiments have S.
3. If $X_2 = 0$, then abort.
4. Estimation of $P_E(K_A = K_B|S)$ based on part of X_2. Alice has key $A_1 \ldots A_{X_3}$ and Bob $B_1 \ldots B_{X_3}$.
5. If $P_E(K_A = K_B|S) < x$, then abort.
6. EC + PA.

QKD as a black-box

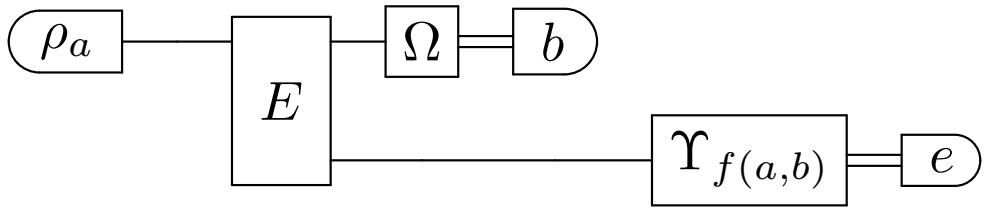
The key is generated by a sequence of independent experiments.
Black-box measures:

- The probability that the protocol will succeed $P_E(S)$.
- The probability of successful key generation $P_E(K_B = K_A|S)$.
- The probability of eavesdropping $P_E(K_E = K_A|S)$.

Eve attacks

1. It is working: $\min_E P_E(S) > 0$.
   - Eve attack: $P_E(S) = 0$, then attack succeeds.
   - Prevention: Define proper QKD.
2. It is useful: $\min_E P_E(K_A = K_B|S) \geq x$.
   - Eve attack: $P_E(K_A = K_B|S) < x$, then attack succeeds.
   - Prevention: Define **Noise resilient Quantum Key Distribution**
3. It is secure: $\max\{P_E(K_E = K_A|S) : P_E(K_A = K_B|S) \geq x\} < x$.
   - Eve attack: $\max\{P_E(K_E = K_A|S) : P_E(K_A = K_B|S) \geq x\} \geq x$, then attack succeeds.
   - Prevention: Define proper value of x.

Noise model



Let ϵ be maximal noise level, then we define

$$y(\epsilon) = \min_{\Phi \in Z_\epsilon} P_\Phi(K_A = K_B|S) \tag{2}$$

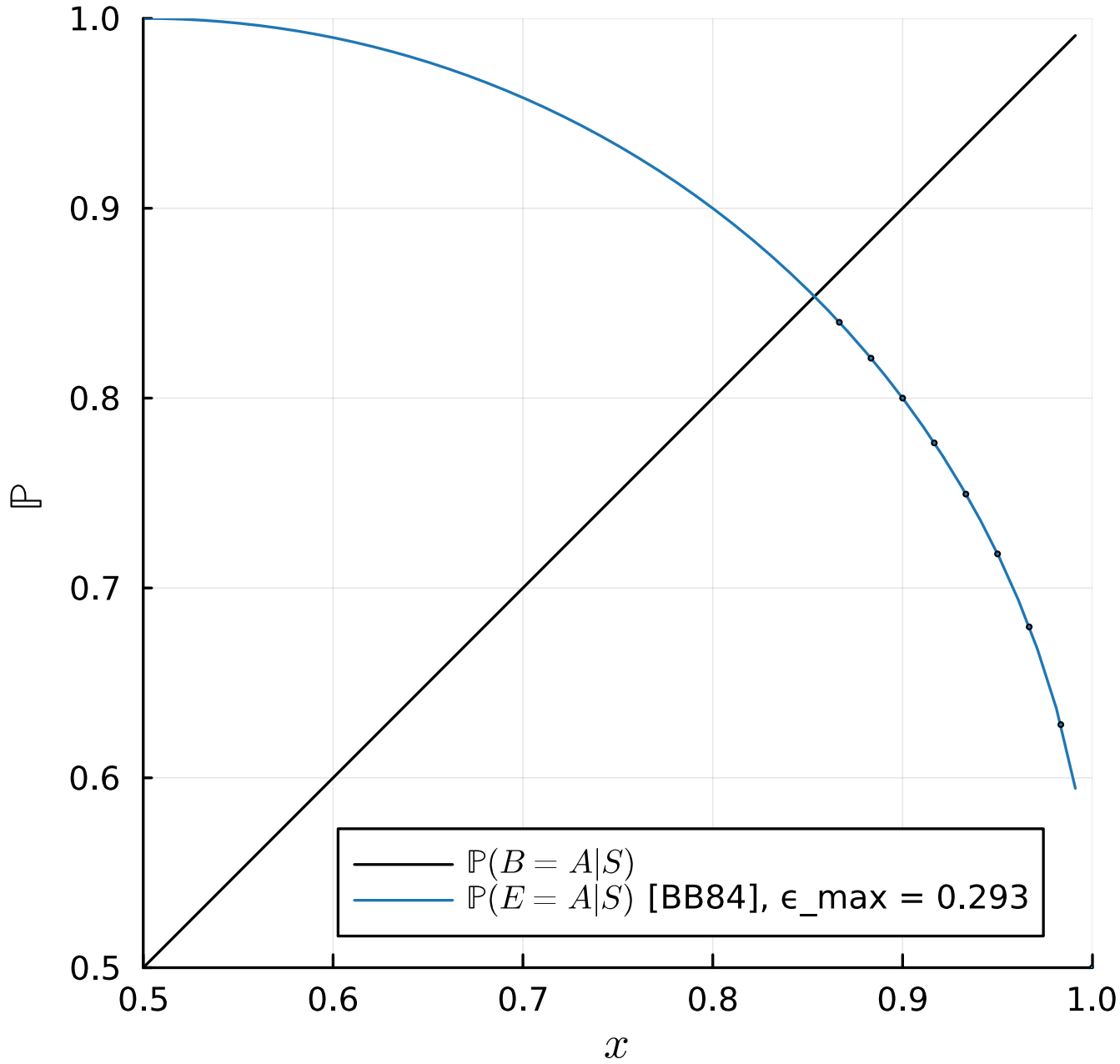
for $\epsilon \in [0,1]$ and $Z_\epsilon = \{\Phi = (1-z)\mathbb{1} + z\Phi_* : z \leq \epsilon\}$

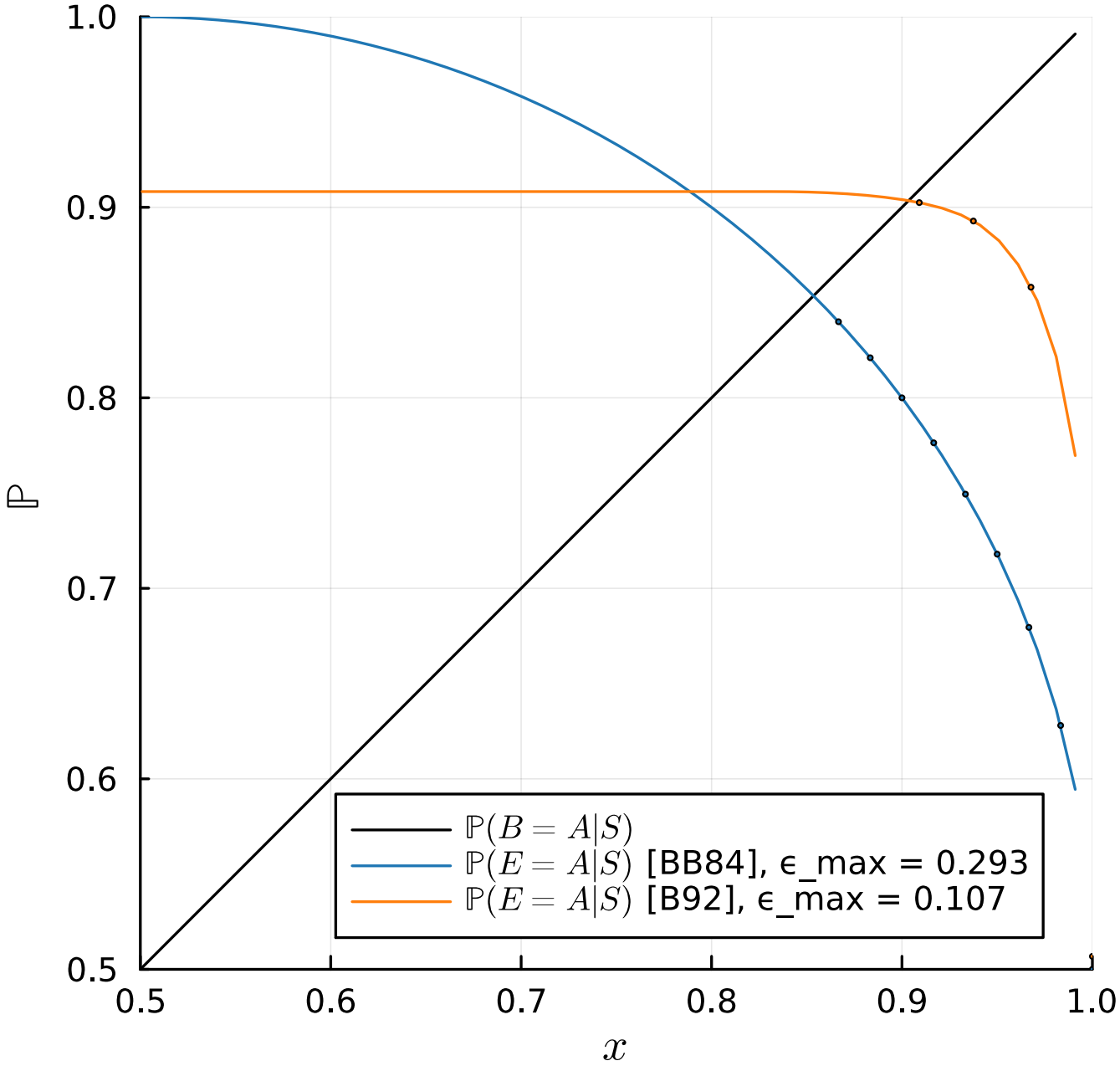
Let x be $1 - \texttt{QBER}$, then we define

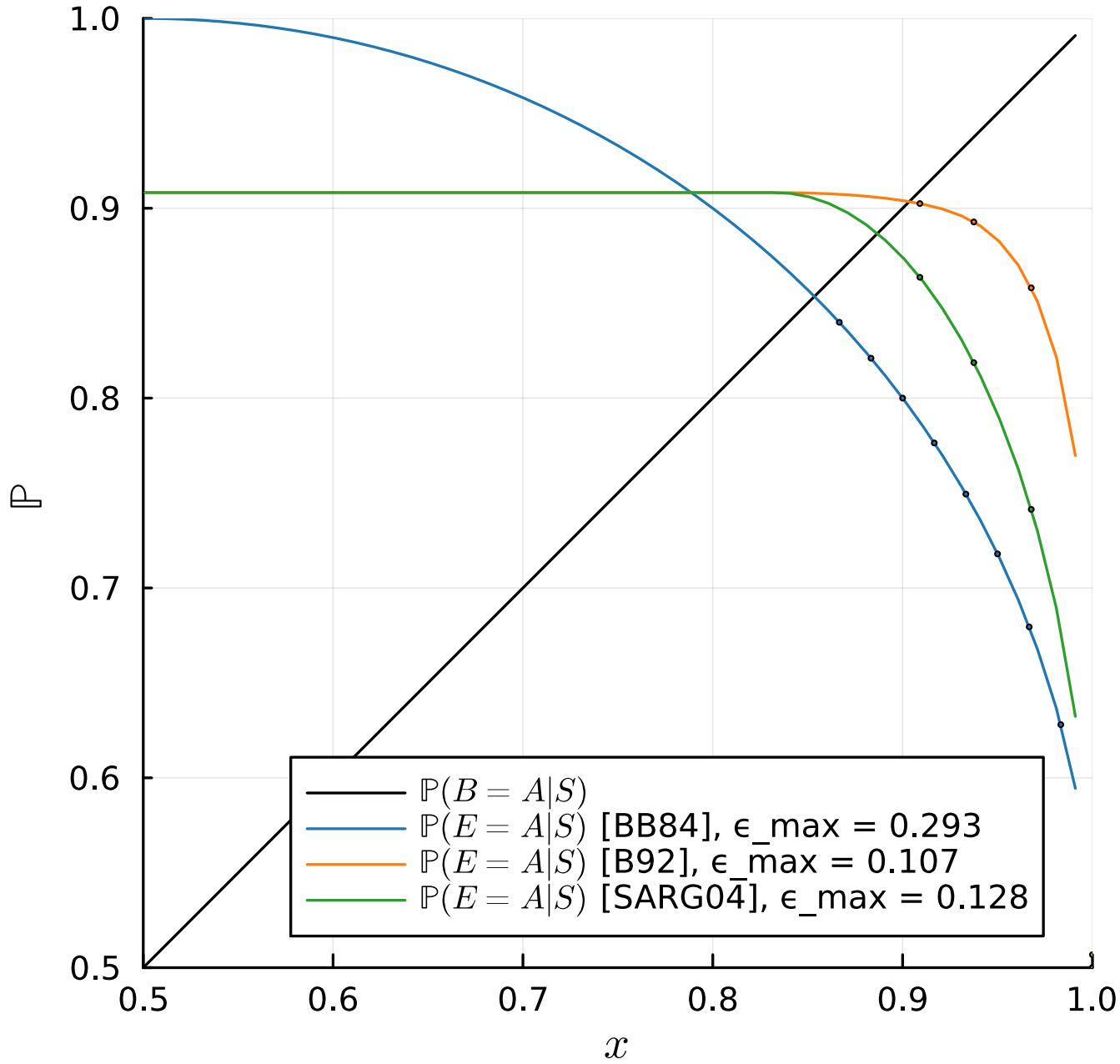
$$y_E(x) = \max\{P_E(K_E = K_A|S) : P_E(K_A = K_B|S) \geq x\} \tag{3}$$

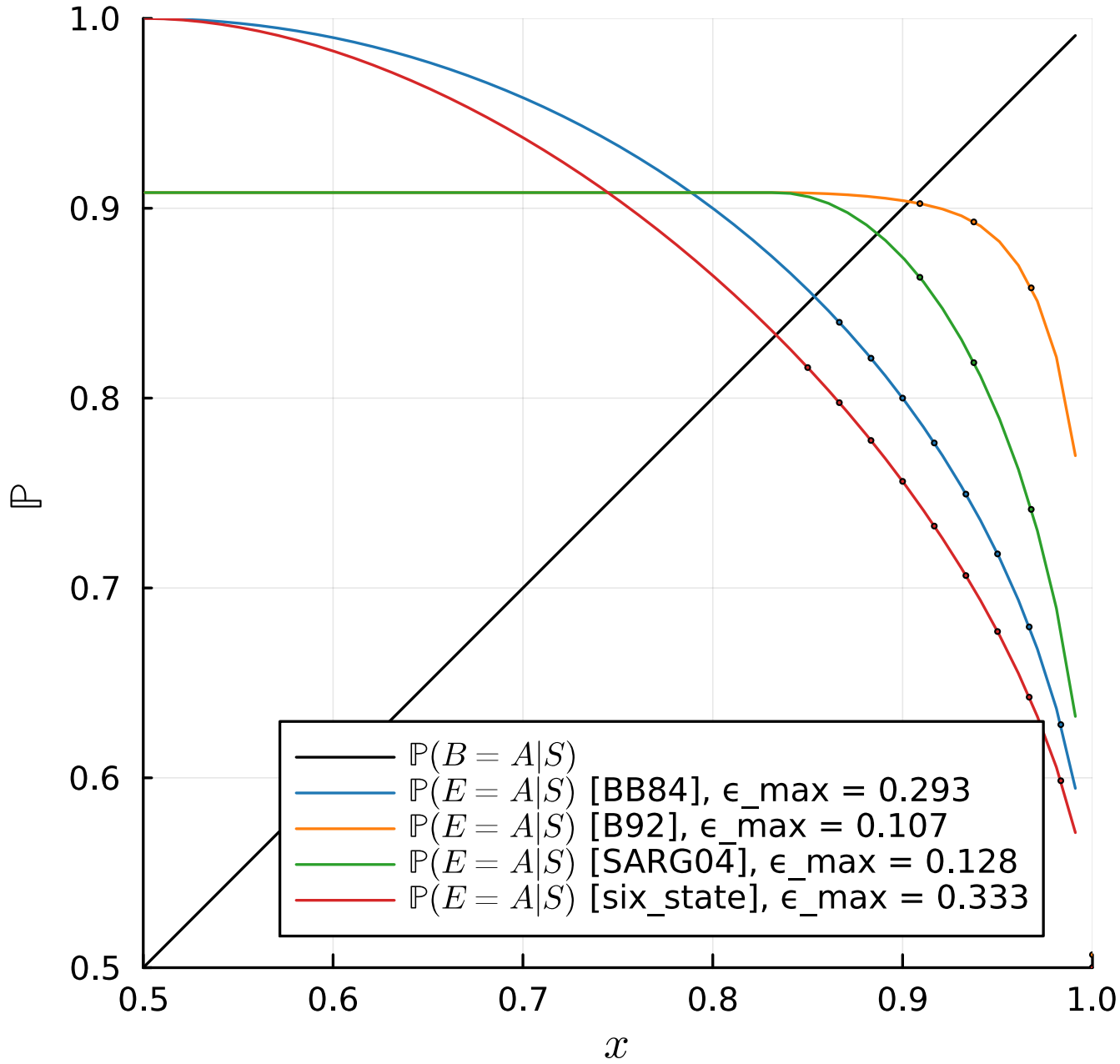
The maximal noise level

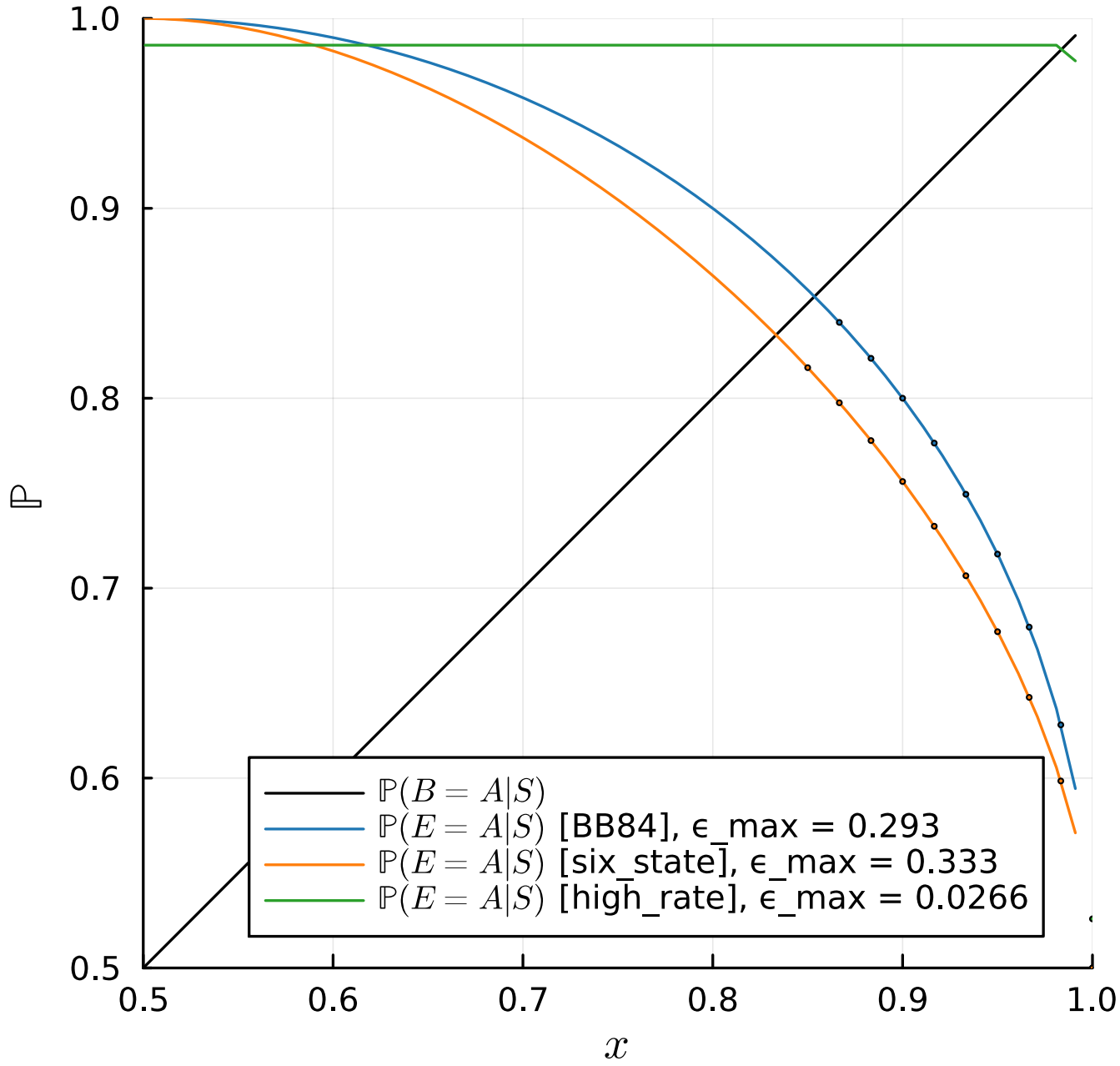
$$\epsilon_{\max} = \sup\{\epsilon \in [0,1] : y(\epsilon) > y_E(y(\epsilon))\} \tag{4}$$

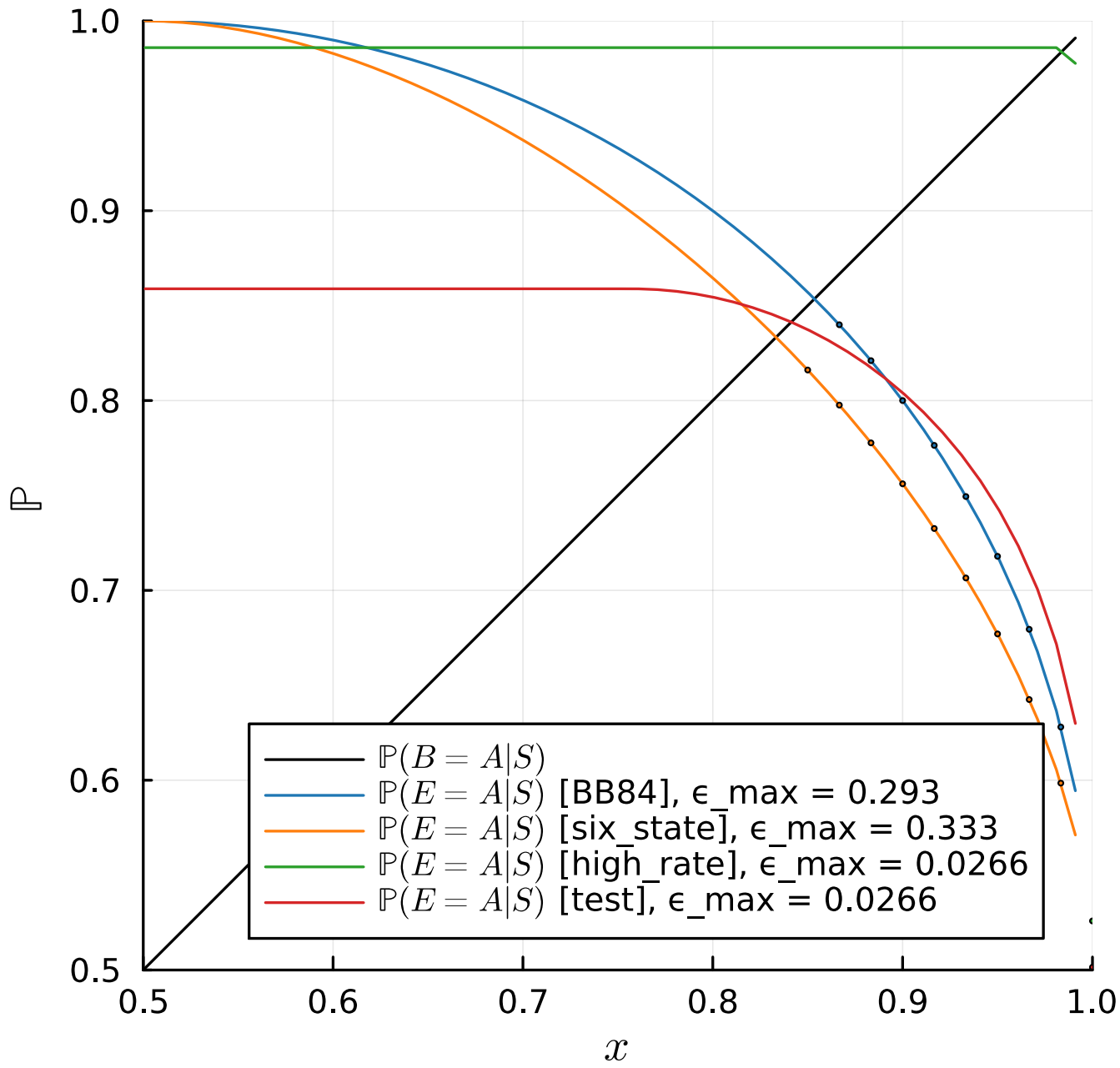

1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293

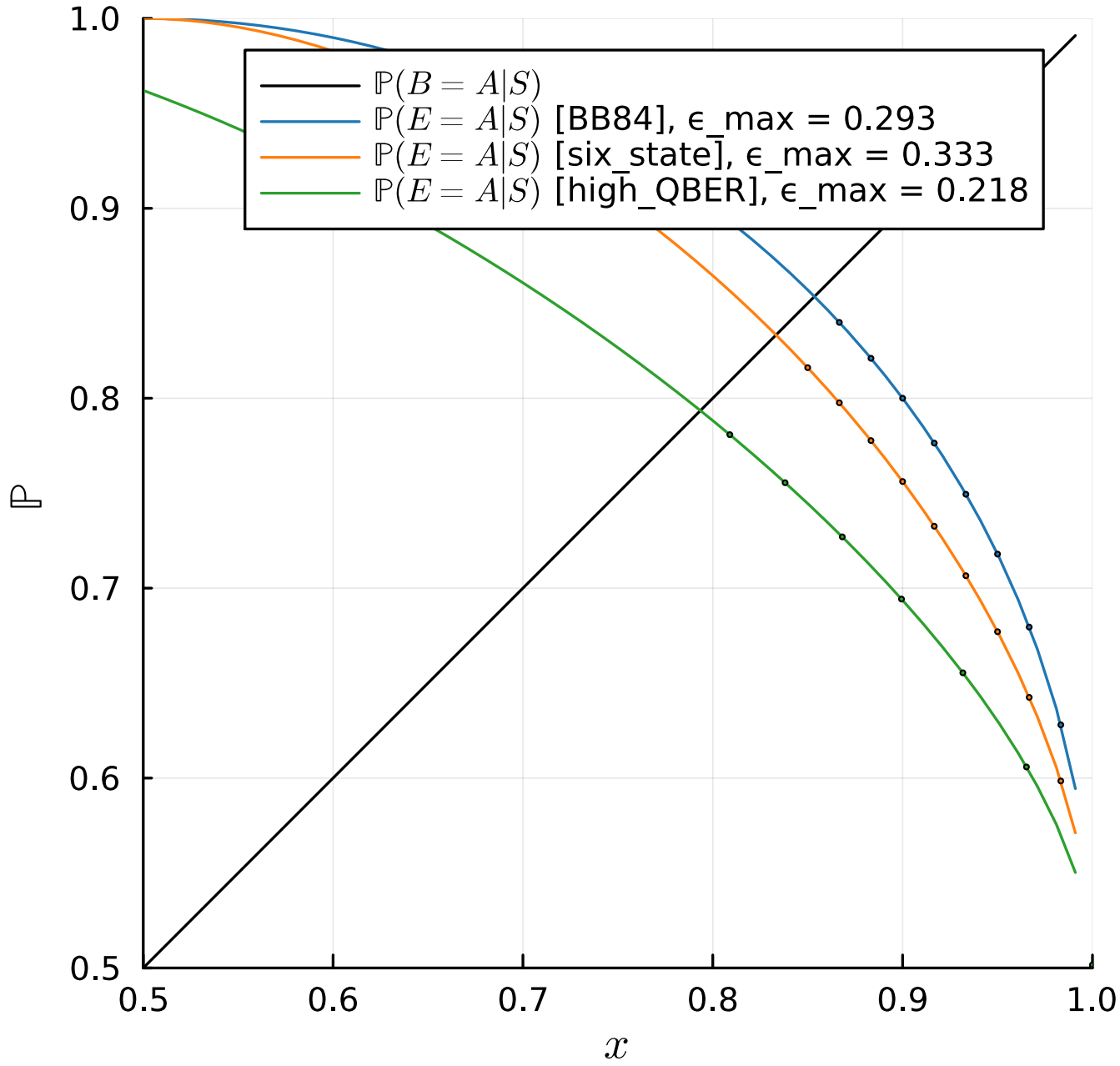

1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [B92], ϵ_max = 0.107


1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [B92], ϵ_max = 0.107
$\mathbb{P}(E = A|S)$ [SARG04], ϵ_max = 0.128


1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [B92], ϵ_max = 0.107
$\mathbb{P}(E = A|S)$ [SARG04], ϵ_max = 0.128
$\mathbb{P}(E = A|S)$ [six_state], ϵ_max = 0.333


1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [six_state], ϵ_max = 0.333
$\mathbb{P}(E = A|S)$ [high_rate], ϵ_max = 0.0266


1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [six_state], ϵ_max = 0.333
$\mathbb{P}(E = A|S)$ [high_rate], ϵ_max = 0.0266
$\mathbb{P}(E = A|S)$ [test], ϵ_max = 0.0266


1.0
0.9
0.8
0.7
0.6
0.5
P
0.5
0.6
0.7
0.8
0.9
1.0
x
$\mathbb{P}(B = A|S)$
$\mathbb{P}(E = A|S)$ [BB84], ϵ_max = 0.293
$\mathbb{P}(E = A|S)$ [six_state], ϵ_max = 0.333
$\mathbb{P}(E = A|S)$ [high_QBER], ϵ_max = 0.218

Thank you for your attention!